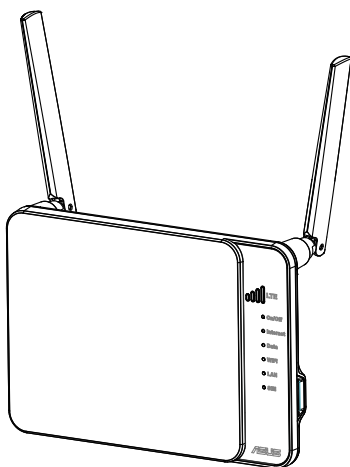


Podręcznik użytkownika

4G-N12

Bezprzewodowy modem router LTE N300



ASUS[®]
IN SEARCH OF INCREDIBLE

Copyright © 2014 ASUSTeK COMPUTER INC. Wszelkie prawa zastrzeżone.

Żadnej z części tego podręcznika, włącznie z opisem produktów i oprogramowania, nie można powielać, przenosić, przetwarzać, przechowywać w systemie odzyskiwania danych lub tłumaczyć na inne języki, w jakiegokolwiek formie lub w jakikolwiek sposób, za wyjątkiem wykonywania kopii zapasowej dokumentacji otrzymanej od dostawcy, bez wyraźnego, pisemnego pozwolenia ASUSTeK COMPUTER INC. ("ASUS").

Gwarancja na produkt lub usługę gwarancyjną nie zostanie wydłużona, jeśli: (1) produkt był naprawiany, modyfikowany lub zmieniany, jeśli wykonane naprawy, modyfikacje lub zmiany zostały wykonane bez pisemnej autoryzacji ASUS; lub, gdy (2) została uszkodzona lub usunięta etykieta z numerem seryjnym.

ASUS UDOSTĘPNIĄ TEN PODRĘCZNIK W STANIE "JAKI JEST", BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI, ZARÓWNO WYRAŹNYCH JAK I DOMNIEMANYCH, WŁĄCZNIE, ALE NIE TYLKO Z DOMNIEMANYMI GWARANCJAMI LUB WARUNKAMI PRZYDATNOŚCI HANDLOWEJ LUB DOPASOWANIA DO OKREŚLONEGO CELU. W ŻADNYM PRZYPADKU FIRMA ASUS, JEJ DYREKTORZY, KIEROWNICY, PRACOWNICY LUB AGENCI NIE BĘDĄ ODPOWIADĄĆ ZA JAKIEKOLWIEK NIEBEZPOŚREDNIE, SPECJANE, PRZYPADKOWE LUB KONSEKWENTNE SZKODY (WŁĄCZNIE Z UTRATĄ ZYSKÓW, TRANSAKCJI BIZNESOWYCH, UTRATĄ MOŻLIWOŚCI KORZYSTANIA LUB UTRACENIEM DANYCH, PRZERWAMI W PROWADZENIU DZIAŁANOŚCI ITP.) NAWET, JEŚLI FIRMA ASUS UPRZEDZAŁA O MOŻLIWOŚCI ZAISTNIENIA TAKICH SZKÓD, W WYNIKU JAKICHKOLWIEK DEFECTÓW LUB BŁĘDÓW W NINIEJSZYM PODRĘCZNIKU LUB PRODUKCIE.

SPECYFIKACJE I INFORMACJE ZNAJDUJĄCE SIĘ W TYM PODRĘCZNIKU, SŁUŻĄ WYŁĄCZNIE CELOM INFORMACYJNYM I MOGĄ ZOSTAĆ ZMIENIONE W DOWOLNYM CZASIE, BEZ POWIADOMIENIA, DLATEGO TEŻ, NIE MOGĄ BYĆ INTERPRETOWANE JAKO WIĄŻĄCE FIRMĘ ASUS DO ODPOWIEDZIALNOŚCI. ASUS NIE ODPOWIADZA ZA JAKIEKOLWIEK BŁĘDY I NIEDOKŁADNOŚCI, KTÓRE MOGĄ WYSTĄPIĆ W TYM PODRĘCZNIKU, WŁĄCZNIE Z OPISANYMI W NIM PRODUKTAMI I OPROGRAMOWANIEM.

Produkty i nazwy firm pojawiające się w tym podręczniku mogą, ale nie muszą być zastrzeżonymi znakami towarowymi lub prawami autorskimi ich odpowiednich właścicieli i używane są wyłącznie w celu identyfikacji lub wyjaśnienia z korzyścią dla ich właścicieli i bez naruszania ich praw.

Spis treści

1	Poznanie routera bezprzewodowego	
1.1	Witamy!.....	5
1.2	Zawartość opakowania.....	5
1.3	Router bezprzewodow.....	6
1.4	Usytuowanie routera	8
1.5	Wymagania dotyczące instalacji	9
1.6	Instalacja routera.....	10
2	Ustawienia sprzętu	
2.1	Logowanie do GUI web.....	12
2.2	QIS z autodetekcją Quick Internet Setup (Szybkie ustawienia połączenia z Internetem)	13
3	Konfiguracja ustawień ogólnych	
3.1	Korzystanie z pozycji Network Map (Mapa sieci)	16
3.2	Wiadomość SMS	16
3.2.1	Nowa wiadomość SMS.....	17
3.2.2	Skrzynka odbiorcza	18
3.2.3	Szkice.....	18
3.2.4	Książka telefoniczna	18
4	Konfiguracja ustawień zaawansowanych	
4.1	Wireless (Sieć bezprzewodowa).....	19
4.1.1	General (Ogólne).....	19
4.1.2	RADIUS Setting (Ustawienia serwera RADIUS).....	22
4.1.3	Wireless MAC Filter (Filtr adresów MAC urządzeń bezprzewodowych).....	23
4.1.4	WPS	24
4.2	LAN (Sieć LAN).....	26
4.2.1	Ustawienia sieci LAN	26
4.2.2	Lista klientów DHCP.....	28
4.3	Sieć WAN	28
4.3.1	Połączenie internetowe	28
4.3.2	Stan połączenia mobilnego	32

Spis treści

4.3.3	Skanowanie połączenia mobilnego.....	34
4.3.4	UPnP	35
4.3.5	Virtual Server/Port Forwarding (Serwer wirtualny/ Przekierowanie portów)	36
4.3.6	DMZ (Strefa DMZ)	37
4.3.7	DDNS (Usługa DDNS).....	39
4.4	Zapora	40
4.4.1	Ogólne	40
4.4.2	Filtr adresów MAC	41
4.4.3	Wykrywanie naruszenia.....	42
4.4.4	Kontrola dostępu	43
4.4.5	Filtr adresów URL	45
4.4.6	Zasada harmonogramu	46
4.5	Administration (Administracja).....	47
4.5.1	System.....	47
4.5.2	Aktualizacja firmware	48
4.5.3	Przywracanie/zapisywanie/przesyłanie ustawień.....	48
4.6	System Log (Dziennik systemu)	49
4.7	Narzędzia sieciowe	50
4.7.1	Ping	50
4.7.2	Traceroute.....	51
4.7.3	Przechwycenie sieci WAN.....	52

5 Często zadawane pytania (FAQ)

Appendices

Notices	56
Informacje kontaktowe producenta.....	69
Informacje o globalnych punktach wsparcia technicznego dla sieci	70

1 Poznanie routera bezprzewodowego

1.1 Witamy!

Dziękujemy za zakupienie bezprzewodowego routera LTE ASUS 4G-N12!

Bezprzewodowy router LTE ASUS 4G-N12 posiada moduł sieciowy 4G, umożliwiający włożenie karty SIM/USIM, w celu uzyskania dostępu i udostępniania połączenia sieciowego 4G LTE lub 3G za pośrednictwem bezpiecznej sieci bezprzewodowej lub dowolnego z czterech gniazd sieciowych. Oferuje on prędkość pobierania danych do 100 Mbps i prędkość wysyłania danych 50 Mbps umożliwiając szybki dostęp do Internetu, płynną transmisję strumieniową multimediiów lub łatwe przesyłanie danych.

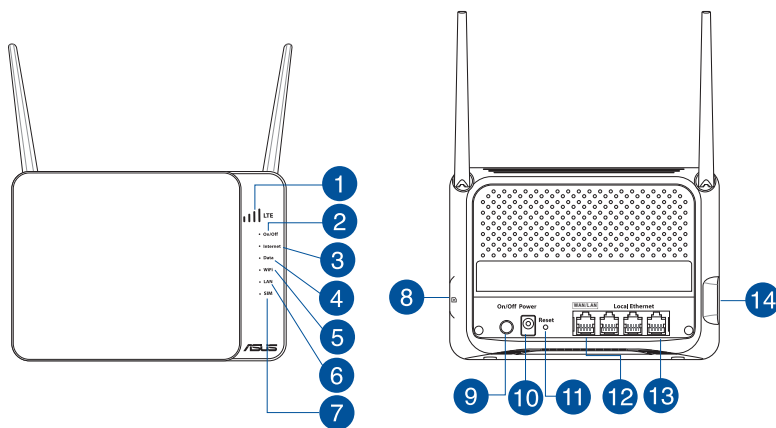
1.2 Zawartość opakowania

- | | |
|---|---|
| <input checked="" type="checkbox"/> 4G-N12 Router bezprzewodowy | <input checked="" type="checkbox"/> Kabel RJ-45 |
| <input checked="" type="checkbox"/> Adapter zasilania | <input checked="" type="checkbox"/> Instrukcja szybkiego uruchomienia |

Uwagi:

- Jeżeli którykolwiek z elementów jest uszkodzony lub brakuje go, skontaktować się z firmą ASUS celem uzyskania pomocy technicznej; patrz lista telefonów pomocy technicznej firmy ASUS na tylnej stronie okładki niniejszej instrukcji obsługi.
 - Zachować oryginalne opakowanie na wypadek skorzystania w przyszłości z usług gwarancyjnych takich jak naprawa lub wymiana.
-

1.3 Router bezprzewodowy



1 LTE Diody siły sygnału sieci LAN 1~4

- 1 zapalona dioda: Bardzo słaby sygnał;
- 2 zapalone diody: Słaby sygnał;
- 3 zapalone diody: Normlany sygnał;
- 4 zapalone diody: Silny sygnał.

2 Dioda zasilania

Wyłączona: Brak zasilania

Włączona: Urządzenie jest gotowe.

3 Dioda Internetu

Wyłączona: Brak połączenia LTE.

Miganie: Nawiązywanie połączenia LTE/Ethernet WAN.

Włączona: Prawidłowe połączenie LTE/Ethernet WAN.

4 Dioda danych (Ruch LTE/Ethernet WAN)

Wyłączona: Brak aktywności przesyłania danych.

Włączona: Połączenie danych jest gotowe.

5 Dioda Wi-Fi


Wyłączona: Brak sygnału 2,4 GHz.

Włączona: System bezprzewodowy jest gotowy.

6 LAN 1~4 LED

Wyłączona: Brak zasilania lub brak fizycznego połączenia z siecią LAN.

Włączona: Fizyczne połączenie z siecią lokalną (LAN).

-
- 7 Dioda karty USIM**
Wyłączona: Brak karty USIM w urządzeniu.
Włączona: Karta USIM jest zainstalowana prawidłowo.
-
- 8 Gniazdo karty USIM**
Do tego gniazda włóż kartę USIM, aby ustawić połączenie LTE WAN.
-
- 9 Przycisk zasilania**
Naciśnij ten przycisk w celu włączenia lub wyłączenia zasilania systemu. 
-
- 10 Power (DC-IN) port**
Insert the bundled AC adapter into this port and connect your router to a power source.
-
- 11 Reset button**
Naciśnij ten przycisk na 5 sekund lub dłużej, aby wyzerować lub przywrócić domyślne ustawienia fabryczne systemu.
-
- 12 Gniazdo sieci WAN/LAN**
Używając kabla Ethernet, połącz gniazdo sieci WAN/LAN routera bezprzewodowego z modemem.
-
- 13 Gniazda LAN**
Służą do podłączania kabli sieciowych celem ustanowienia lokalnego połączenia sieciowego.
-
- 14 Przycisk WPS**
Przycisk służy do uruchamiania kreatora WPS.
-

Uwagi:

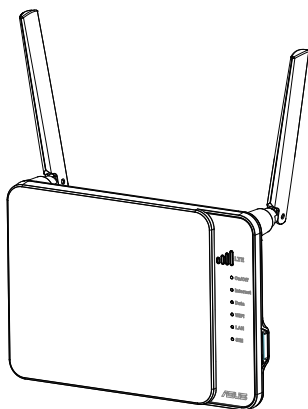
- Stosować tylko zasilacz dołączony do zestawu. Zastosowanie innych zasilaczy może spowodować uszkodzenie urządzenia.
- Pamiętaj o włożeniu karty SIM do gniazda karty, przed włączeniem zasilania routera.
- **Dane techniczne:**

Zasilacz sieciowy prądu stałego	Wyjście prądu stałego: +12 V przy prądzie maks. 1 A		
Temperatura pracy	0~40°C	Przechowywanie	0~70°C
Wilgotność działania	50~90%	Przechowywanie	20~90%

1.4 Usytuowanie routera

Dla zapewnienia najlepszej transmisji sygnału bezprzewodowego pomiędzy routerem bezprzewodowym a podłączonymi urządzeniami sieciowymi należy upewnić się, że:

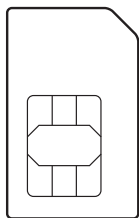
- Umieścić bezprzewodowy router LTE w pobliżu okna, aby odbierać sygnał LTE z najwyższą jakością, zapewniając maksymalną prędkość wysyłania do stacji bazowej LTE.
- Urządzenie trzymać z dala od metalowych przeszkód oraz bezpośredniego działania promieniowania słonecznego.
- Nie ustawiać bezprzewodowego routera LTE w zapyłonym lub wilgotnym środowisku.
- W celu zapobiegnięcia zakłóceniom lub utratom sygnału trzymać urządzenie z dala od urządzeń Wi-Fi obsługujących wyłącznie pasma 802.11g lub 20 MHz, komputerowych urządzeń peryferyjnych 2,4 GHz, urządzeń Bluetooth, telefonów bezprzewodowych, transformatorów, silników do wysokich obciążeń, świetlówek, kuchenek mikrofalowych, lodówek oraz innego wyposażenia przemysłowego.
- Zawsze zaktualizować oprogramowanie do najnowszej wersji oprogramowania sprzętowego. Najnowsze informacje dotyczące aktualizacji oprogramowania można uzyskać na stronie internetowej ASUS pod adresem <http://www.asus.com>.
- Aby zapewnić najlepszy sygnał bezprzewodowy należy ukierunkować trzy odłączane anteny jak na ilustracji poniżej.



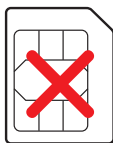
1.5 Wymagania dotyczące instalacji

Do wykonania ustawień sieci bezprzewodowej, należy spełnić następujące wymagania:

- Karta mini SIM/USIM z subskrypcją WCDMA i LTE



Mini SIM card



Micro SIM card



Nano SIM card

UWAGA: Standardowa karta SIM/USIM jest standardowa karta mini SIM.

WAŻNE! Upewnij się, że karta SIM/USIM posiada subskrypcję usług WCDMA i LTE. W celu uzyskania informacji o tych usługach skontaktuj się z dostawcą usług mobilnych.

OSTRZEŻENIE! W routerze można używać tylko standardowej karty SIM/USIM. Użycie innej karty SIM, takiej jak mikro lub nano SIM, może spowodować uszkodzenie routera.

- Modem ADSL/kablowy z subskrypcją Internetu
- Komputer z gniazdem Ethernet RJ-45 (LAN) (10Base-T/100Base-TX) lub kartą sieciową Wi-Fi z interfejsem bezprzewodowym 2,4 GHz 802.11 b/g/n
- Przeglądarka sieciowa, taka jak Internet Explorer, Firefox, Safari lub Google Chrome

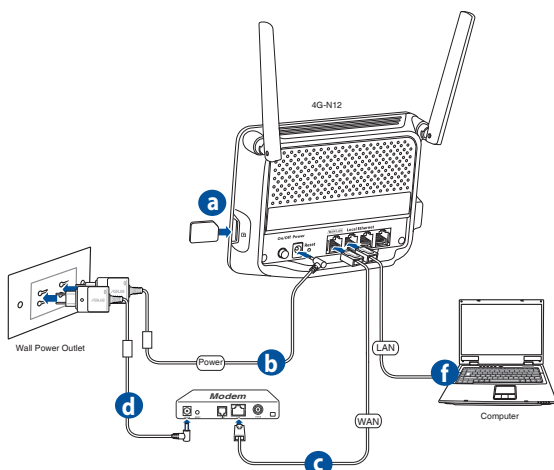
Uwagi:

- Jeśli komputer nie posiada wbudowanej obsługi sieci bezprzewodowej, w celu połączenia z siecią WLAN, można zainstalować w komputerze adapter WLAN IEEE 802.11a/b/g/n/
 - Nie podłączaj wtyczki telefonu do gniazda RJ-45. Może to spowodować uszkodzenie bezprzewodowego routera LTE.
 - Kable Ethernet RJ-45 wykorzystywane do połączenia z urządzeniami sieciowymi nie powinny być dłuższe niż 100 metrów.
-

1.6 Instalacja routera

UWAGA!

- Unikaj instalowania bezprzewodowego routera LTE podczas burzy. Istnieje wtedy zagrożenie porażenia prądem elektrycznym z wyładowania atmosferycznego.
 - Nie próbuj rozbierać lub ponownie składać urządzenia. Manipulowanie bezprzewodowym routerem LTE może spowodować unieważnienie gwarancji.
 - Podczas mocowania lub czyszczenia urządzenia, pamiętaj aby odłączyć wtyczkę przewodu zasilającego od bezprzewodowego routera LTE.
 - Podczas przenoszenia bezprzewodowego routera LTE miej suche ręce, aby uniknąć porażenia prądem elektrycznym.
-



- a. Włóż kartę SIM/USIM do gniazda karty USIM.
- b. Podłącz kabel zasilacza prądu przemiennego routera do gniazda DC-IN i włóż zasilacz do gniazodka sieciowego.
- c. Używając kabla sieciowego połącz modem z gniazdem WAN/LAN routera bezprzewodowego.
- d. Podłącz kabel zasilacza prądu przemiennego modemu do gniazda DC-IN i włóż zasilacz do gniazodka sieciowego.
- e. Włącz router.
- f. Używając dostarczonego w zestawie kabla sieciowego połącz komputer z gniazdem LAN routera.
- g. W celu ręcznego połączenia z siecią bezprzewodową:
 1. Włącz funkcję Wi-Fi klienta sieci bezprzewodowej, aby automatycznie wyszukać sieci bezprzewodowe.
 2. Wybierz sieć bezprzewodową o nazwie "ASUS", która jest domyślnym identyfikatorem SSID sieci bezprzewodowych routerów ASUS.
 3. Po wyświetleniu monitu, wpisz domyślne hasło routera, które znajduje się na naklejce umieszczonej z tyłu routera.



2 Ustawienia sprzętu

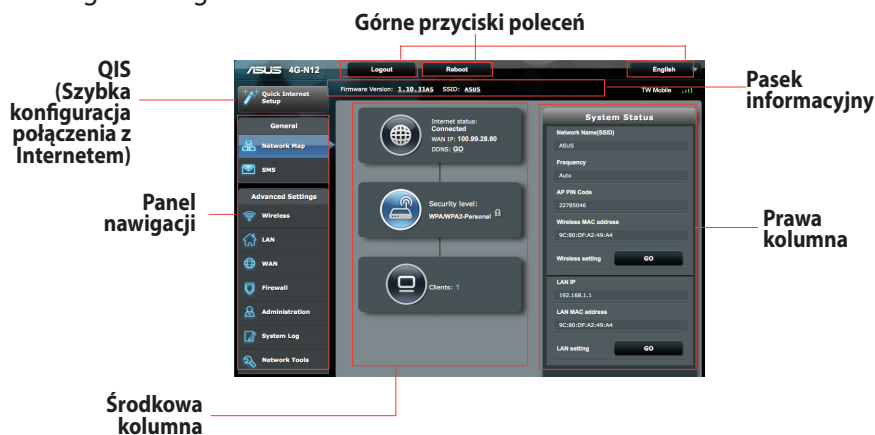
2.1 Logowanie do GUI web

Router bezprzewodowy ASUS jest dostarczany z intuicyjnym GUI (graphics user interface (graficzny interfejs użytkownika)), który umożliwia łatwą konfigurację jego różnych funkcji poprzez przeglądarkę sieci web, taką jak Internet Explorer, Firefox, Safari lub Google Chrome.

UWAGA: Funkcje mogą się różnić w zależności od wersji oprogramowania sprzętowego.

Aby zalogować się do GUI web:

1. W przeglądarce sieci web, takiej jak Internet Explorer, Firefox, Safari lub Google Chrome, ręcznie wprowadź domyślny adres IP routera bezprzewodowego: **192.168.1.1**, lub wprowadź <http://router.asus.com>.
2. Na stronie logowania wprowadź domyślną nazwę użytkownika (**admin**) i hasło (**admin**).
3. Można rozpocząć konfigurację różnych ustawień routera bezprzewodowego firmy ASUS za pomocą sieciowego interfejsu graficznego.



UWAGI:

- Domyślnym hasłem logowania jest **admin**. Możesz ręcznie ustawić nowe hasło zawierające od 3 do 16 znaków alfanumerycznych z rozróżnianiem małych i dużych liter.
- Jeżeli połączenie z siecią WAN nie jest gotowe, zostanie automatycznie skierowany na stronę Quick Internet Setup (QIS).

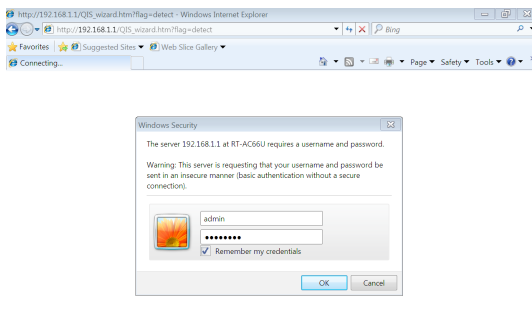
2.2 QIS z autodetekcją Quick Internet Setup (Szybkie ustawienia połączenia z Internetem)

Funkcja QIS (Quick Internet Setup (Szybkie ustawienia połączenia z Internetem)) pomaga w szybkim wykonaniu połączenia z Internetem.

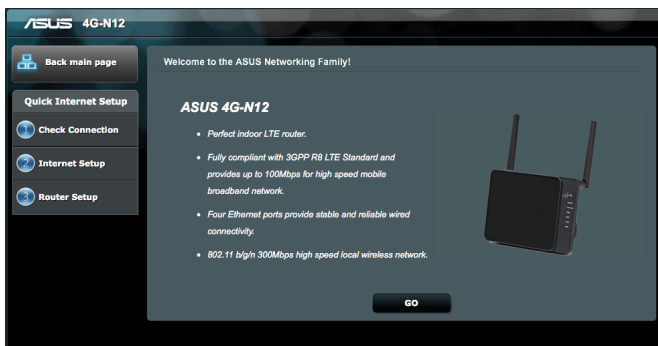
Uwagi: Podczas ustawiania połączenia z Internetem **pierwszy raz**, naciśnij i przytrzymaj **przycisk Reset** na routerze bezprzewodowym w celu przywrócenia jego ustawień fabrycznych.

Aby użyć QIS z autodetekcją:

1. Zaloguj się do sieciowego interfejsu graficznego. Automatycznie wyświetlona zostanie strona QIS (Szybka konfiguracja połączenia z Internetem).



2. Na ekranie powitania kliknij polecenie **Go (Wejdz)**, aby kontynuować.

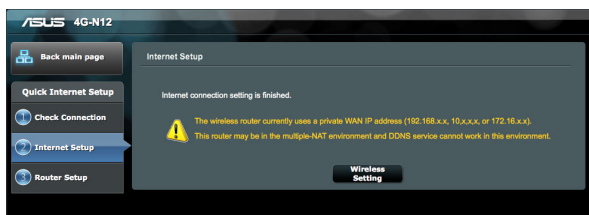


3. Zmień hasło routera bezprzewodowego. Po wykonaniu, kliknij **check (Dalej)**.

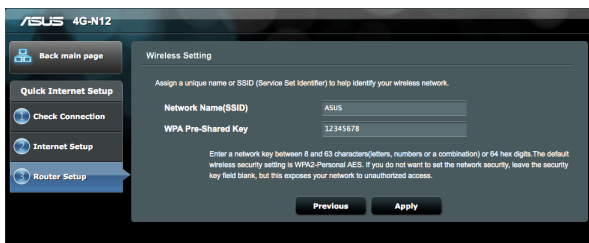
UWAGA: Zalecamy wpisanie unikalnego hasła administratora w celu ochrony sieci przed złośliwymi atakami.



4. Router bezprzewodowy automatycznie wykrywa i stosuje ustawienia APN. Po wykonaniu, kliknij przycisk **WLAN Setting (Ustawienia WLAN)** w celu skonfigurowania ustawień bezprzewodowej sieci lokalnej.



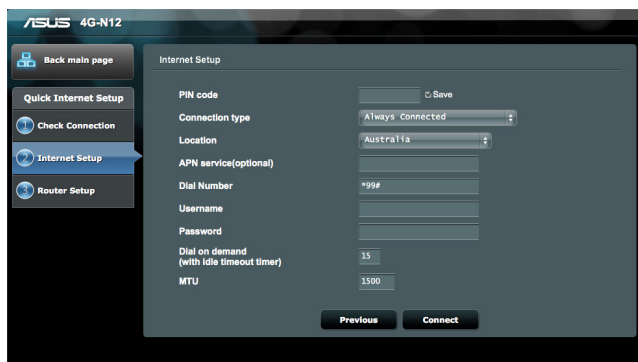
5. Przypisz unikalną nazwę sieci (SSID) i klucz bezpieczeństwa sieci. Po wykonaniu, kliknij przycisk **Apply (Zastosuj)**.



6. Wyświetlone zostaną ustawienia połączenia z Internetem oraz dane dotyczące połączenia bezprzewodowego. Aby kontynuować kliknij **Next (Dalej)**.



7. Jeżeli kreator nie zastosuje ustawień APN lub wymagane jest podanie kodu PIN karty SIM, musisz ręcznie zakończyć wykonywanie szerokopasmowego połączenia z siecią mobilną. Wpisz konieczne ustawienia APN i kod PIN karty SIM. Po wykonaniu, kliknij przycisk **Connect (Połącz)**.



UWAGA: Automatyczne wykrywanie połączenia ISP jest wykonywane przy pierwszej konfiguracji routera bezprzewodowego lub po zresetowaniu routera bezprzewodowego do ustawień domyślnych.

3 Konfiguracja ustawień ogólnych

3.1 Korzystanie z pozycji Network Map (Mapa sieci)

Pozycja Network Map (Mapa sieci) umożliwia sprawdzenie statusu połączenia internetowego, konfigurowanie ustawień zabezpieczeń sieci i zarządzanie klientami sieciowymi.

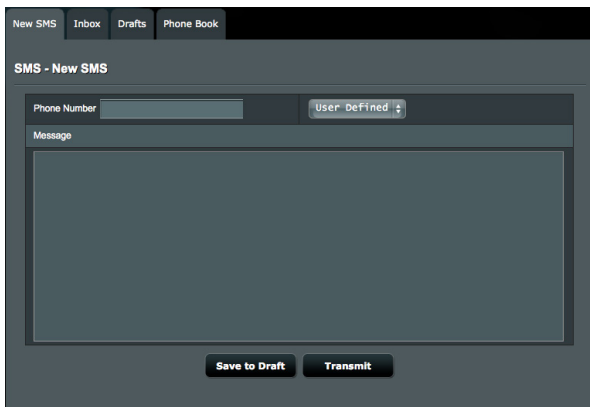


3.2 Wiadomość SMS

SMS (Short Message Service) jest usługą przesyłania wiadomości tekstowych umożliwiającą wysyłanie i odbieranie wiadomości od lub przez Twój router bezprzewodowy.

3.2.1 Nowa wiadomość SMS

Funkcja ta umożliwia wysyłanie krótkich wiadomości z Twojego routera bezprzewodowego.



Wysyłanie nowej wiadomości SMS:

1. Wpisz numer telefonu odbiorcy.
2. Napisz wiadomość.
3. Kliknij przycisk **Transmit (Wyślij)**, aby wysłać wiadomość.

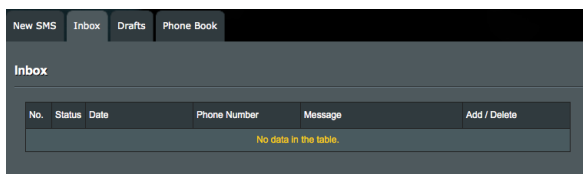
Zapisanie szkicu wiadomości SMS:

1. Wpisz numer telefonu odbiorcy.
2. Napisz wiadomość.
3. Kliknij przycisk **Save to Draft (Zapisz do Szkice)**, aby zapisać szkic wiadomości.

3.2.2 Skrzynka odbiorcza

Skrzynka odbiorcza umożliwia przeglądanie odebranych SMS zapisanych w urządzeniu.

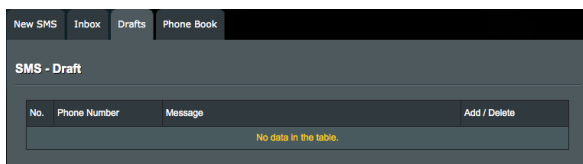
Kliknij przycisk **Read (Czytaj)**, aby przeczytać wiadomości lub kliknij przycisk **Delete (Usuń)**, aby usunąć wiadomość.



3.2.3 Szkice

Widoczne tutaj są wszystkie szkice wiadomości zapisane w bezprzewodowym routerze LTE.

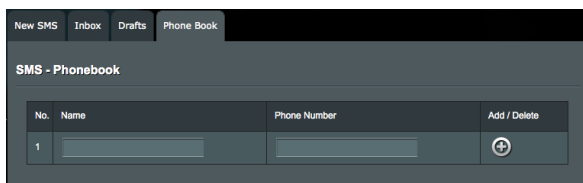
Kliknij przycisk **Transmit (Wyślij)**, aby wysłać wiadomość lub kliknij przycisk **Delete (Usuń)**, aby usunąć wiadomość.



3.2.4 Książka telefoniczna

Książka telefoniczna umożliwia zapisanie często używanych numerów telefonów.

Aby dodać numer telefonu wpisz nazwę i numer telefonu i kliknij



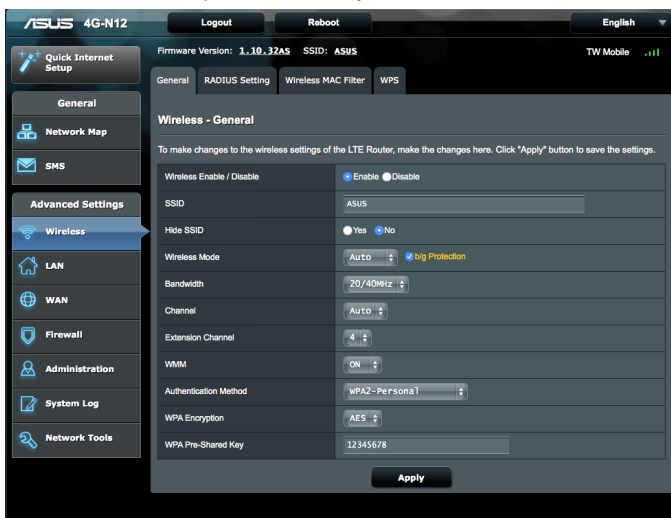
4 Konfiguracja ustawień zaawansowanych

4.1 Wireless (Sieć bezprzewodowa)

Bezprzewodowy router LTE działa jako bezprzewodowy punkt dostępowy, umożliwiając urządzeniom bezprzewodowym łączyć się z Internetem. Graficzny interfejs użytkownika umożliwia skonfigurowanie kanału radiowego, identyfikatora SSID, bezpieczeństwa i ustawień WPS.

4.1.1 General (Ogólne)

Zakładka General (Ogólne) umożliwia konfigurację podstawowych ustawień sieci bezprzewodowej.



W celu skonfigurowania podstawowych ustawień sieci bezprzewodowej:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Wireless (Sieć bezprzewodowa) > wybierz zakładkę General (Ogólne)**.
2. **Wireless Enable / Disable (Włącz / Wyłącz sieć bezprzewodową):** Wybierz opcję **(Enable) Włącz**, aby wykorzystywać router jako bezprzewodowy punkt dostępowy.

3. Przypisz unikatową nazwę identyfikatora SSID (Service Set Identifier) lub sieci zawierającą maksymalnie 32 znaki w celu identyfikacji sieci bezprzewodowej. Urządzenia Wi-Fi będą identyfikować sieć bezprzewodową i łączyć się z nią za pomocą przypisanego identyfikatora SSID. Identyfikatory SSID widoczne na pasku informacyjnym są aktualizowane po zapisaniu nowych identyfikatorów SSID w ustawieniach.
4. W polu **Hide SSID (Ukryj SSID)** wybierz opcję **Yes (Tak)**, aby nie dopuścić do wykrywania identyfikatora SSID przez urządzenia bezprzewodowe. Po włączeniu tej funkcji konieczne będzie ręczne wprowadzanie identyfikatora SSID w urządzeniu bezprzewodowym w celu zapewnienia jego dostępu do sieci bezprzewodowej.
5. Wybierz jedną z dostępnych opcji trybu sieci bezprzewodowej w celu określenia typów urządzeń bezprzewodowych, które będą mogły łączyć się z routerem bezprzewodowym:
 - **Automat.:** Wybierz opcję **Auto (Automat.)**, aby z routerem bezprzewodowym mogły łączyć się urządzenia 802.11AC, 802.11n, 802.11g i 802.11b.
 - **Starsze:** Wybierz opcję **Legacy (Starsze)**, aby z routerem bezprzewodowym mogły łączyć się urządzenia 802.11b/g/n. Urządzenia obsługujące natywnie tryb 802.11n będą jednak działać wyłącznie z maksymalną szybkością 54 Mb/s.
 - **Tylko N:** Wybierz opcję **N only (Tylko N)**, aby zmaksymalizować wydajność sieci bezprzewodowej w standardzie N. Ustawienie to sprawia, że z routerem bezprzewodowym nie będą łączyć się urządzenia 802.11g ani 802.11b.
 - **b/g Protection (Ochrona b/g):** W większości sytuacji, najlepsza charakterystyka uzyskiwana jest przy wyłączonym trybie chronionym sieci bezprzewodowej. Jeżeli korzystasz z routera w środowisku o dużym ruchu 802.11b, 802.11g lub o dużych zakłóceniach, włącz tę funkcję, aby uzyskać najlepszą charakterystykę przepustowości dla 802.11n.
6. Wybierz jedno z dostępnych pasm kanału w celu uwzględnienia większych szybkości transmisji:
 - 40MHz:** Wybierz to pasmo, aby zmaksymalizować przepływność w sieci bezprzewodowej.
 - 20MHz (default) [20MHz (domyślne)]:** Wybierz to pasmo w przypadku występowania problemów z połączeniem

bezprzewodowym.

7. Wybierz kanał działania routera bezprzewodowego. Wybierz opcję **Auto (Automat.)**, aby router bezprzewodowy automatycznie wybierał najmniej zakłócony kanał.
8. **Extension Channel (Kanał rozszerzenia)**: Kanał rozszerzenia, który możesz przypisać oparty jest o następujące założenia:
 - Kiedy szerokość pasma ustawiona jest na 20 MHz, kanał rozszerzenia jest wyłączony.
 - Kiedy kanał bezprzewodowy (kanał główny) ustawiony jest na 1, wybierz kanał 5 jako kanał rozszerzony.
 - Kiedy kanał bezprzewodowy ustawiony jest na 9, wybierz kanał 5 lub 13 jako kanał rozszerzony.
9. **WMM**: Włączenie lub wyłączenie korzystania z QoS. Funkcja QoS (Quality of Service) umożliwia różnicowanie ruchu WMM (Wi-Fi Multimedia) i nadaniem u najwyższego priorytetu usługi przekazywania.
10. Wybierz jedną z dostępnych metod uwierzytelniania:
 - **Otwarty system**: Ta opcja nie zapewnia zabezpieczeń.
 - **WPA/WPA2 Personal/WPA Auto-Personal**: Ta opcja zapewnia mocne zabezpieczenia. Można korzystać z zabezpieczenia WPA (z TKIP) lub WPA2 (z AES). Po wybraniu tej opcji konieczne jest korzystanie z szyfrowania TKIP + AES i wprowadzenie hasła WPA (klucza sieciowego).
 - **WPA/WPA2 Enterprise/WPA Auto-Enterprise**: Ta opcja zapewnia bardzo mocne zabezpieczenia. Jest ona dostępna z zintegrowanym serwerem EAP lub zewnętrznym serwerem uwierzytelniania RADIUS z wewnętrzną bazą danych.
11. Po zakończeniu kliknij przycisk **Apply (Zastosuj)**.

UWAGA: Router bezprzewodowy obsługuje maksymalną szybkość transmisji 54 Mb/s po ustawieniu dla pozycji **Wireless Mode (Tryb sieci bezprzewodowej)** opcji **Auto (Automat.)** i wybraniu metody szyfrowania **WEP** lub **TKIP**.

4.1.2 RADIUS Setting (Ustawienia serwera RADIUS)

Pozycja RADIUS (Remote Authentication Dial In User Service) Setting (Ustawienia serwera RADIUS) zapewnia dodatkową warstwę zabezpieczeń w przypadku wybrania metody uwierzytelniania WPA-Enterprise, WPA2-Enterprise lub Radius with 802.1x (Radius z 802.1x).

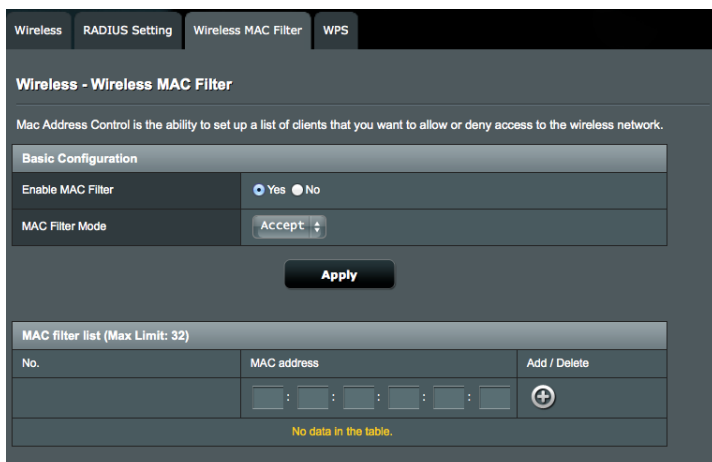
The screenshot shows the 'Wireless - RADIUS Setting' configuration page. At the top, there are four tabs: 'General', 'RADIUS Setting' (which is selected), 'Wireless MAC Filter', and 'WPS'. Below the tabs, the title 'Wireless - RADIUS Setting' is displayed. A descriptive text states: 'This section allows you to set up additional parameters for authorizing wireless clients through RADIUS server. It is required while you select "Authentication Method" in "Wireless - General" as "WPA-Enterprise/ WPA2-Enterprise/ Radius with 802.1x".' Below this text is a form with four fields: 'Server IP Address' with the value '0.0.0.0', 'Server Port' with the value '1812', 'Connection Secret' which is empty, and 'Network Key Rotation Interval' with the value '2000' and a unit '(seconds)' to its right. At the bottom of the form is an 'Apply' button.

W celu skonfigurowania ustawień serwera RADIUS w sieci bezprzewodowej:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Wireless (Sieć bezprzewodowa)** > wybierz zakładkę **RADIUS Setting (Ustawienia serwera RADIUS)**.
2. **Server IP Address (Adres IP serwera):** W tym polu wpisz adres IP serwera RADIUS.
3. **Server Port (Port serwera):** W tym polu wpisz numer portu serwera RADIUS.
4. **Connection Secret (Tajne połączenie):** Wpisz hasło, aby uzyskać dostęp do Twojego serwera RADIUS.
5. **Network Key Rotation Interval (Odstęp rotacji klucza sieci):** Definiuje okres odnowienia, w którym serwer RADIUS wysyła do wszystkich klientów nowy klucz szyfrowania.
6. Po zakończeniu, kliknij przycisk **Apply (Zastosuj)**.

4.1.3 Wireless MAC Filter (Filtr adresów MAC urządzeń bezprzewodowych)

Pozycja Wireless MAC Filter (Filtr adresów MAC urządzeń bezprzewodowych) zapewnia kontrolę nad pakietami przesyłanymi na określony adres MAC (Media Access Control) w danej sieci bezprzewodowej.



Wireless RADIUS Setting Wireless MAC Filter WPS

Wireless - Wireless MAC Filter

Mac Address Control is the ability to set up a list of clients that you want to allow or deny access to the wireless network.


Basic Configuration

Enable MAC Filter ☒ Yes ☐ No

MAC Filter Mode **Accept**

Apply

MAC filter list (Max Limit: 32)

No.	MAC address	Add / Delete
		
No data in the table.		

W celu skonfigurowania filtra adresów MAC urządzeń bezprzewodowych:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane)** > **Wireless (Sieć bezprzewodowa)** > wybierz zakładkę **Wireless MAC Filter (Filtr adresów MAC urządzeń bezprzewodowych)**.
2. W polu **Frequency (Częstotliwość)** wybierz pasmo częstotliwości, które ma być używane dla pozycji Wireless MAC Filter (Filtr adresów MAC urządzeń bezprzewodowych).
3. Z listy rozwijanej **MAC Filter Mode (Tryb filtra adresów MAC)** wybierz opcję **Accept (Akceptuj)** lub **Reject (Odrzuć)**.
 - Wybierz opcję **Accept (Akceptuj)**, aby urządzenia z listy MAC filter list (Lista filtrowanych adresów MAC) mogły łączyć się z siecią bezprzewodową.
 - Wybierz opcję **Reject (Odrzuć)**, aby urządzenia z listy MAC filter list (Lista filtrowanych adresów MAC) nie mogły łączyć się z siecią bezprzewodową.
4. W obszarze MAC filter list (Lista filtrowanych adresów MAC) kliknij przycisk **Add (Dodaj)**  i wprowadź adres MAC urządzenia bezprzewodowego.
5. Kliknij przycisk **Apply (Zastosuj)**.

4.1.4 WPS

WPS (Wi-Fi Protected Setup) umożliwia łatwe utworzenie bezpiecznej sieci bezprzewodowej z użyciem kodu PIN lub funkcji sterowania przyciskiem (PBC).

Wireless

RADIUS Setting

Wireless MAC Filter

WPS

WPS

Wi-Fi Protected Setup (WPS) is the industry standard method to simplify the security setup and management of Wi-Fi networks. You now can easily set up and connect to a WPA-enabled 802.11 network with WPS-certificated devices using either Personal Information Number (PIN) or Push Button Configuration (PBC) method. Legacy devices without WPS can be added to the network using the traditional manual configuration method.

Enable WPS (WPS)

Enabled

Apply

Personal Information Number (PIN) Method : Key in the router's PIN code in the client's WPS utility and configure the network name and security settings.

Client PIN Code

Enroll

Key in the router's PIN code in the client's WPS utility and configure the network name and security settings.

AP PIN Code : 22785046

Generate PIN

Restore PIN

Przewiń w dół, aby wyświetlić pozostałe pozycje:

Push Button Configuration (PBC) Method : Push and hold PBC button on your wireless router for 3 seconds or click "Start PBC". Then start PBC on the device you want to connect to the wireless router within two minutes.

Start PBC

Manual Configuration Method : For client devices without WPS, manually configure the device with the following settings.

Network Name(SSID)	ASUS
Wireless Security	Configured
Authentication	WPA2+PSK
WPA Encryption	AES
Network Key	12345678

W celu włączenia funkcji WPS w sieci bezprzewodowej:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Wireless (Sieć bezprzewodowa) > wybierz zakładkę WPS.**
2. W polu **Enable WPS (Włącz funkcję WPS)**, wybierz **Enabled (Włączona)**, a następnie kliknij przycisk **Apply (Zastosuj)**.
3. Skonfiguruj WPS korzystając z metody z kodem PIN lub PBC. Szczegółowe informacje znajdują się w opisach kolejnych etapów.

Konfiguracja WPS z zastosowaniem metody kodu PIN:

1. Włącz zasilanie urządzenia klienckiego obsługującego metodę WPS z kodem PIN (Personal Information Number).
2. Wpisz kod PIN urządzenia klienckiego i kliknij przycisk **Enroll (Zapisz na liście)**.

UWAGA: Kod PIN można znaleźć albo na spodzie obudowy, albo na interfejsie użytkownika urządzenia klienckiego.

3. Uruchom na urządzeniu klienckim proces WPS PIN.

UWAGA: Szczegółowe informacje można znaleźć w podręczniku użytkownika urządzenia klienckiego.

4. Jeżeli chcesz zmienić kod PIN routera, kliknij przycisk **Generate PIN (Generuj PIN)** lub **Restore PIN (Przywróć PIN)**, aby utworzyć nowy lub przywrócić domyślny kod PIN.

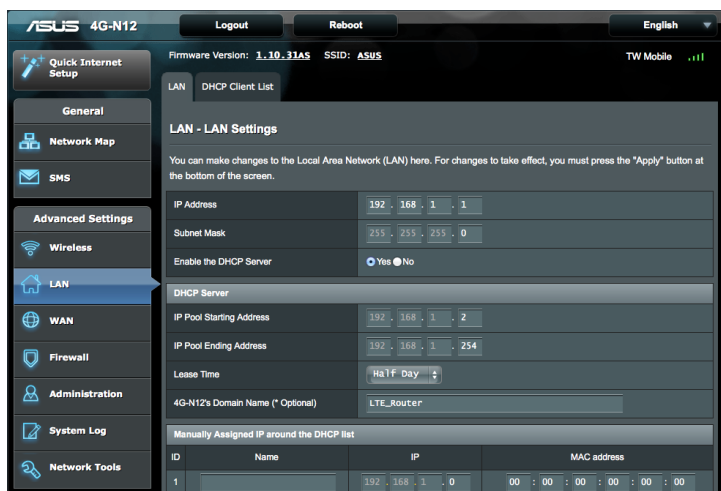
Konfiguracja WPS z zastosowaniem metody PBC:

1. Włącz zasilanie urządzenia klienckiego obsługującego WPS.
2. Na ekranie WPS routera bezprzewodowego kliknij przycisk **Start PBC (Uruchom PBC)**. Możesz również nacisnąć przycisk WPS z lewej strony routera bezprzewodowego.
3. Naciśnij przycisk WPS na urządzeniu klienckim.

4.2 LAN (Sieć LAN)

4.2.1 Ustawienia sieci LAN

Ekran ustawień sieci LAN umożliwia skonfigurowanie adresu IP sieci lokalnej dla routera LTE oraz zmodyfikowanie ustawień serwera DHCP.



W celu zmodyfikowania ustawień adresu IP sieci LAN:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > LAN (Sieć LAN)** > wybierz zakładkę **LAN IP (Adres IP sieci LAN)**.
2. Wprowadź adresy IP i maski podsieci routera bezprzewodowego.
3. W polu **Enable the DHCP Server (Włącz serwer DHCP)** zaznacz pozycję **Yes (Tak)** lub **No (Nie)**. Domyślnie, funkcja Serwer DHCP jest włączona.
4. W polu **IP Pool Starting Address (Adres początkowy zakresu IP)**, wprowadź adres początkowy IP.
5. W polu **IP Pool Ending Address (Adres końcowy zakresu IP)**, wprowadź adres końcowy IP.

UWAGI:

- Zalecamy, podczas określania zakresu adresów IP, stosowanie formatu adresów IP: 192.168.1.xxx (xxx może być dowolną liczbą pomiędzy 2 a 254).
- Pozycja IP Pool Starting Address (Adres początkowy zakresu IP) nie powinna być wyższa niż pozycja IP Pool Ending Address (Adres końcowy zakresu IP).

6. Na liście rozwijalnej **Lease Time (Czas dzierżawy)** wybierz harmonogram, według którego będzie wygasać przypisany adres IP. Po upływie określonego harmonogramu, serwer DHCP przypisuje nowy adres IP.

Statyczny DHCP jest użyteczną funkcją umożliwiającą powiązanie określonego urządzenia klienckiego ze statycznym adresem IP w sieci LAN. Adres IP na serwerze DHCP zostanie zarezerwowany dla unikalnego adresu MAC urządzenia klienckiego DHCP stosownie do ustawień wykonanych poniżej.

Manually Assigned IP around the DHCP list									
ID	Name	IP				MAC address			
1		192	168	1	0	00	: 00	: 00	: 00
2		192	168	1	0	00	: 00	: 00	: 00
3		192	168	1	0	00	: 00	: 00	: 00
4		192	168	1	0	00	: 00	: 00	: 00
5		192	168	1	0	00	: 00	: 00	: 00
6		192	168	1	0	00	: 00	: 00	: 00
7		192	168	1	0	00	: 00	: 00	: 00
8		192	168	1	0	00	: 00	: 00	: 00
9		192	168	1	0	00	: 00	: 00	: 00
10		192	168	1	0	00	: 00	: 00	: 00

4.2.2 Lista klientów DHCP

Ekran Lista klientów DHCP wyświetla informacje o klientach DHCP. Kliknij przycisk **Refresh (Odśwież)**, aby zaktualizować listę podłączonych klientów.

LAN DHCP Client List			
LAN - DHCP Client List			
This page shows you the IP address, Host Name and MAC address of each computer that is connected to your network. If the computer does not have a host name specified, then the Host Name field will be blank. Pressing "Refresh" will update the list.			
IP Address	Host Name(optional):	MAC address	Expiry time
192.168.1.2	Vincent5-C-NB2	00:26:4A:1D:2C:7C	11:49:00
Refresh			

4.3 Sieć WAN

Router LTE posiada wbudowany moduł LTE (Long Term Evolution). Sieć LTE oferuje szerokie pasmo przepustowości kanałów, od 5 MHz do 20 MHz, oraz duże prędkości przesyłania danych mobilnych, do 50 Mbps przy wysyłaniu i do 100 Mbps przy pobieraniu.

Obsługiwane pasma pokazane są poniżej:

- Pasma LTE: FDD B3/7/20
 - LTE Cat. 3: Pobieranie: 100 Mbps, Wysyłanie: 50 Mbps
- UMTS: B1/8
 - HSPA +: Pobieranie: 42 Mbps, Wysyłanie: 5,76 Mbps

4.3.1 Połączenie internetowe

Konfiguracja ustawień połączenia internetowego:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > WAN (Sieć WAN)** > wybierz zakładkę **Internet Connection (Połączenie internetowe)**.
2. W polu **WAN Type (Typ sieci WAN)** wybierz **LTE/UMTS** lub **WAN**.

- **Typ sieci WAN - LTE/UMTS**

WAN - Internet Connection

4G-N12 supports several connection types to WAN (wide area network). These types are selected from the dropdown menu beside WAN Connection Type. The setting fields differ depending on the connection type you selected.

WAN Index

WAN Type: **LTE/UMTS**

Mobile Broadband

PIN code: ☒ Save
No SIM Card

Connection type: **Always Connected**

Location: **Auto**

APN service(optional): **internet**

Dial Number: ***99#**

Username:

Password:

Dial on demand (with idle timeout timer): **15**

MTU: **1500**

Apply

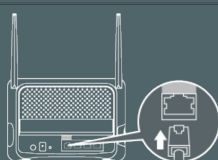
- Skonfiguruj następujące pozycje:
 - **PIN Code (Kod PIN):** Wpisz kod PIN dostawcy 3G/4G.
 - **Connection Type (Typ połączenia):** Pole to umożliwia zdefiniowanie polityk połączenia. Zalecamy wybranie opcji **Auto-Triggered by traffic (Auto – Uruchamiane przez ruch)**, w przypadku korzystania z usługi transmisji danych o przepustowości mniejszej od potrzebnej.
 - **Location (Lokalizacja):** Wybierz lokalizację dostawcy usług 3G/4G z listy rozwijanej.
 - **APN services (Usługi APN) (opcjonalnie):** Wpisz tutaj informacje usługi APN (nazwa punktu dostępowego). W celu uzyskania szczegółowych informacji skontaktuj się z dostawcą usług 3G/4G.
 - **Dial Number (Wybierz numer):** Wpisz numer dostępowy dostawcy 3G/4G do połączenia.

- **Username (Nazwa użytkownika)/Password (Hasło):** Wpisz nazwę użytkownika i hasło zapewniane przez operatora sieci 3G/4G.
 - **Dial on demand (with idle timeout timer) (Wybieranie numeru na życzenie (z zegarem czasu oczekiwania):** Wprowadź czas (w minutach), po którym router przechodzi w tryb uśpienie w przypadku braku aktywności w sieci.
 - **MTU:** Służy do ustawienia parametru MTU (maksymalny rozmiar wysyłanego pakietu).
- b. Kliknij przycisk **Apply (Zastosuj)**, aby połączyć z siecią 3G/4G. Stan połączenia będzie wyświetlany na ekranie **Mobile Connection Status (Stan połączenia mobilnego)**.

UWAGA: Kod PIN różni się w zależności od dostawcy.

• Typ sieci WAN - sieć WAN

4G-N12 supports several connection types to WAN (wide area network). These types are selected from the dropdown menu beside WAN Connection Type. The setting fields differ depending on the connection type you selected.

WAN Index	
WAN Type	WAN ↕
	
Basic Config	
WAN Connection Type	Automatic IP ↕
Enable WAN	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable NAT	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable UPnP	UPnP_FAQ <input type="radio"/> Yes <input checked="" type="radio"/> No
WAN DNS Setting	
Connect to DNS Server automatically	<input type="radio"/> Yes <input checked="" type="radio"/> No
Account Setting	
Authentication	None ↕
Special Requirement from ISP	
Host Name	<input type="text"/>
MAC Address	<input type="text"/> MAC Clone
Apply	


- a. Skonfiguruj poniższe ustawienia. Po zakończeniu, kliknij przycisk **Apply (Zastosuj)**.
- **WAN Connection Type (Typ połączenia WAN):** Wybierz typ połączenia udostępniany przez usługodawcę internetowego. Dostępne opcje to **Automatic IP (Automatyczny adres IP)**, **PPPoE**, **PPTP**, **L2TP** lub **fixed IP (Stały adres IP)**. W przypadku braku pewności co do typu połączenia WAN lub braku możliwości uzyskania przez router prawidłowego adresu IP należy skontaktować się z usługodawcą internetowym.
 - **Enable WAN (Włącz sieć WAN):** Wybierz opcję **Yes (Tak)**, aby router mógł uzyskać dostęp do Internetu. Wybierz opcję **No (Nie)**, aby wyłączyć dostęp do Internetu.
 - **Enable NAT (Włącza NAT):** Translator adresów sieciowych NAT (Network Address Translation) to system, w którym jeden publiczny adres IP (adres IP sieci WAN) jest używany do zapewniania dostępu do Internetu klientom sieciowym o prywatnym adresie IP w sieci LAN. Prywatny adres IP każdego klienta sieciowego jest zapisywany w tabeli NAT i używany do rozsyłania przychodzących pakietów danych.
 - **Łączenie z serwerem DNS:** Umożliwia automatyczne uzyskiwanie adresu IP serwera DNS przez router od usługodawcy internetowego. DNS to host w Internecie, który tłumaczy nazwy internetowe na numeryczne adresy IP.
 - **Uwierzytelnianie:** Ta pozycja może być określana przez niektórych usługodawców internetowych. Jeśli to konieczne, sprawdź u usługodawcy internetowego i wprowadź.
 - **Nazwa hosta:** W tym polu można wprowadzić nazwę hosta danego routera. Jest to zwykle specjalny wymóg usługodawcy internetowego. Jeśli usługodawca internetowy przypisał nazwę hosta do komputera, wprowadź ją w tym polu.
 - **Adres MAC:** Pozycja MAC (Media Access Control) address (Adres MAC) to unikatowy identyfikator urządzenia

sieciowego. Niektórzy usługodawcy internetowi monitorują adresy MAC urządzeń sieciowych, które łączą się z ich usługą i odrzucają wszelkie próby połączeń urządzeń nierozpoznanych. Aby uniknąć problemów z połączeniami spowodowanych niezarejestrowanym adresem MAC, można:

- Skontaktować się z usługodawcą internetowym i zaktualizować adres MAC skojarzony z jego usługą.
- Sklonować lub zmienić adres MAC routera bezprzewodowego firmy ASUS w celu jego dopasowania do adresu MAC poprzedniego urządzenia sieciowego rozpoznawanego przez usługodawcę internetowego.

4.3.2 Stan połączenia mobilnego

Ekran Stan połączenia mobilnego wyświetla szczegółowe informacje o stanie szerokopasmowego połączenia mobilnego.

Internet Connection	Mobile Connection Status	Mobile Connection Scan	UPnP	Virtual Server / Port Forwarding	DMZ	DDNS
WAN - Mobile Connection Status						
Mobile Broadband-LTE Status						
Strength						
Status	Available (Voice & Data)					
ISP	TW Mobile(46697) LTE					
Connection time	20 min. 37 sec.					
Total downstream transmitting traffic	1.27 MBytes.					
Total upstream transmitting traffic	1.2 MBytes.					
Current downstream transmitting rate	6.36 Kbps.					
Current upstream transmitting rate	6.73 Kbps.					
Version Info						
version	20130328_1KGQCL_4036_M0.11					
IMEI	352056050004999					
IMS	466977100295254					
Data Usage						
Data traffic limit	<input checked="" type="radio"/> Enable <input type="radio"/> Disable					
Your operator's data usage accounting may differ.						
Apply						

Przewiń w dół, aby wyświetlić pozostałe pozycje:

Data Usage	
Data traffic limit	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Data usage cycle	Oct 1 - Oct 31
Data usage limit	0 (MB)
Data Usage	About 1 MB is used, as measured by the wireless router.

Your operator's data usage accounting may differ.

Apply

W celu konfiguracji ustawień opcji Wykorzystanie danych:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane)** > **WAN (Sieć WAN)** i wybierz zakładkę **Mobile Connection Status (Stan połączenia mobilnego)**.
2. **Limit transferu danych:** Wybierz opcję **Włącz**, aby umożliwić ustawienie limitu wykorzystania połączenia internetowego.
3. **Limit wykorzystania danych:** Umożliwia ustawienie górnego miesięcznego limitu wykorzystania połączenia z Internetem. Kiedy wykorzystanie danych dojdzie do limitu, dostęp do Internetu zostanie zablokowany.
4. Kliknij przycisk **Apply (Zastosuj)**.

4.3.3 Skanowanie połączenia mobilnego

Internet Connection Mobile Connection Status Mobile Connection Scan UPnP Virtual Server / Port Forwarding DMZ DDNS

WAN - Internet Connection

Preferred network type ☒ Auto ☐ 2G Only ☐ 3G Only ☐ 4G Only

Select	ISP	Status	Operator Service
SIM is not detected.			

Scan

Apply

Wybór preferowanego mobilnego połączenia szerokopasmowego:

1. W polu **Preferred network type (Preferowany typ sieci)** wybierz pasmo częstotliwości UMTS.
2. Kliknij przycisk **Scan (Skanuj)**, aby pokazać wszystkie dostępne sieci komórkowe.
3. Wybierz sieć komórkową i kliknij przycisk **Apply (Zastosuj)** w celu nawiązania połączenia.

UWAGI:

- Router LTE Router może wykrywać ISP w oparciu o informacje IMSI karty SIM. Jeżeli sieć komórkowa twojego dostawcy ISP nie zostanie znaleziona, podłącz się do sieci roamingowej innego ISP.
 - Korzystanie z usługi roamingu spowoduje naliczenie dodatkowych opłat. Dowiedz się u swojego dostawcy ułóg komórkowych przed skorzystaniem z usługi roamingu.
-

4.3.4 UPnP

Protokół UPnP (Universal Plug and Play) umożliwia sterowanie kilkoma urządzeniami (takimi jak routery, telewizory, zestawy stereo, konsole do gier i telefony komórkowe) w sieci z obsługą adresów IP ze sterowaniem centralnym za pomocą bramy lub bez niego. Protokół UPnP łączy komputery dowolnego typu, zapewniając bezproblemowe połączenie sieciowe do konfiguracji zdalnej i przesyłania danych. Podczas korzystania z protokołu UPnP nowe urządzenie sieciowe jest wykrywane automatycznie. Po połączeniu z siecią, urządzenia można skonfigurować zdalnie w celu zapewnienia obsługi aplikacji P2P, gier interaktywnych, konferencji wideo oraz serwerów sieciowych lub proxy. W przeciwieństwie do przekierowania portów, które wymaga ręcznej konfiguracji ustawień portów, protokół UPnP automatycznie konfiguruje router w celu zapewnienia przyjmowania połączeń przychodzących i bezpośrednich żądań do określonego komputera w sieci lokalnej.

Internet Connection	Mobile Connection Status	Mobile Connection Scan	UPnP	Virtual Server / Port Forwarding	DMZ	DDNS
WAN - UPnP						
UPnP (Universal Plug and Play) allows several devices (routers, televisions, stereo systems, game consoles, cellular phone) to be controlled via an IP-based network with or without a central control through a gateway.						
General						
UPnP		<input checked="" type="radio"/> Enable <input type="radio"/> Disable				
Apply						

4.3.5 Virtual Server/Port Forwarding (Serwer wirtualny/Przekierowanie portów)

Serwer wirtualny to metoda kierowania ruchu sieciowego z Internetu przychodzącego na określony port lub zakres portów do urządzenia lub urządzeń w sieci lokalnej.

Jeżeli skonfigurujesz router LTE jako serwer wirtualny, zdalni użytkownicy uzyskujący dostęp do usług takich jak sieć lub FTP w sieci lokalnej za pośrednictwem publicznych adresów IP będą automatycznie przekierowywani na serwery lokalne skonfigurowane z prywatnymi adresami IP. Innymi słowy, zależnie od wymaganej usługi (numer portu TCP/UDP), router LTE przekierowuje zewnętrzne żądania usług do odpowiednich serwerów (posiadających inne wewnętrzne adresy IP).

Internet Connection Mobile Connection Status Mobile Connection Scan UPnP Virtual Server / Port Forwarding DMZ

WAN - Virtual Server / Port Forwarding

Virtual Server / Port forwarding allows remote computers to connect to a specific computer or service within a private network (LAN). For better connection, some P2P applications (such as BitTorrent), may also require that you set forwarding setting. Please refer to the P2P application's user manual for details. You can open the multiple port forwarding ports in router and redirect data through those ports to a single client on your network.

If you want to specify a Port Range for clients on the same network, enter the Service Name, the Port Range (e.g. 192.168.1.1-192.168.1.254) and the Local Port empty.

Add Active worlds Add

Clear entry 1 Clear Clear All

Enable	Description	Port Range	Protocol	Local IP
<input type="checkbox"/>			TCP	192.168.1.
<input type="checkbox"/>			TCP	192.168.1.
<input type="checkbox"/>			TCP	192.168.1.
<input type="checkbox"/>			TCP	192.168.1.
<input type="checkbox"/>			TCP	192.168.1.
<input type="checkbox"/>			TCP	192.168.1.
<input type="checkbox"/>			TCP	192.168.1.

Przykładowo, jeżeli ustawisz Typ/Port publiczny na TCP/80 (Http lub sieć) i Prywatny IP/Port na 192.168.2.2:80, wówczas wszystkie żądania HTTP od użytkowników zewnętrznych będą przekierowywane na 192.168.2.2 na port 80. Dlatego, przez wprowadzeniu adresu IP dostarczonego przez ISP, użytkownicy Internetu mogą uzyskać dostęp do potrzebnych usług z lokalnego adresu, do którego ich przekierowałeś.

UWAGA: Najbardziej typowe porty usługi TCP obejmują: HTTP: 80, FTP: 21, Telnet: 23 i POP3: 110. Lista portów znajduje się na stronie <http://www.iana.org/assignments/port-numbers>.

4.3.6 DMZ (Strefa DMZ)

W wirtualnej strefie DMZ dostęp do Internetu ma jeden klient, który odbiera wszystkie pakiety przychodzące do danej sieci lokalnej.

Ruch przychodzący z Internetu jest zwykle odrzucany i kierowany do określonego klienta tylko wtedy, gdy w danej sieci skonfigurowane zostało przekierowanie portów lub wyzwalamie portów. W przypadku konfiguracji strefy DMZ tylko jeden klient sieciowy odbiera wszystkie pakiety przychodzące.

Skonfigurowanie strefy DMZ w sieci jest przydatne, jeśli porty przychodzące mają być otwarte lub w przypadku hostowania serwera domeny, sieci Web lub poczty e-mail.

Przestroga: Otwarcie wszystkich portów klienta na ruch z Internetu naraża sieć na ataki z zewnątrz. Należy wziąć pod uwagę zagrożenia bezpieczeństwa związane z korzystaniem ze strefy DMZ.

Internet Connection

Mobile Connection Status

Mobile Connection Scan

UPnP

Virtual Server / Port Forwarding

DMZ

DDNS


WAN - DMZ

Virtual DMZ allows you to expose one computer to the Internet, so that all the inbounds packets will be redirected to the computer you set. It is useful while you run some applications that use uncertain incoming ports. Please use it carefully.

The computer in the DMZ is not protected from hacker attacks.

To put a computer in the DMZ, enter the last digits of its IP address in the field below and select "Enable". Click "Apply" for the change to take effect.

Enable DMZ			
	Static IP	Local IP	Enable
1	100.121.79.231	192.168.1.0	<input type="checkbox"/>



The wireless router currently uses a private WAN IP address (192.168.x.x, 10.x.x.x, or 172.16.x.x).

This router may be in the multiple-NAT environment and DNS service cannot work in this environment.

Apply

W celu skonfigurowania strefy DMZ:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane)** > **WAN (Sieć WAN)** > wybierz zakładkę **DMZ (Strefa DMZ)**.
2. Skonfiguruj poniższe ustawienia. Po zakończeniu kliknij przycisk **Apply (Zastosuj)**.
 - **Enable DMZ (Włącz strefę DMZ):** Wprowadź ostatnią cyfrę adresu IP sieci LAN klienta, który będzie obsługiwał usługę strefy DMZ i będzie miał dostęp do Internetu. Klient serwera musi mieć statyczny adres IP. Zaznacz opcję **Enable (Włącz)**.

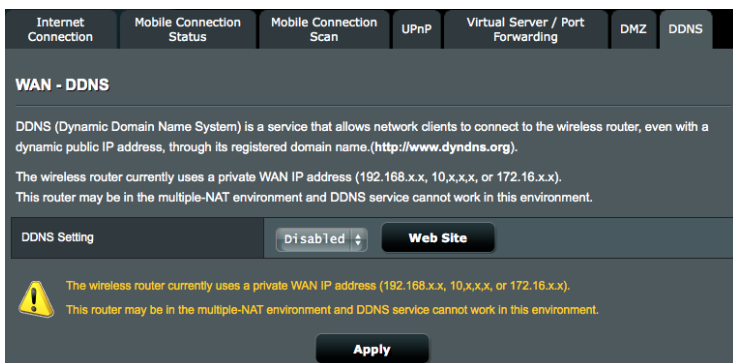
W celu usunięcia strefy DMZ:

1. Usuń zaznaczenie opcji **Enable (Włącz)**, a następnie kliknij przycisk **Apply (Zastosuj)**.

4.3.7 DDNS (Usługa DDNS)

Skonfigurowanie usługi DDNS (Dynamic Domain Name System) umożliwia uzyskiwanie dostępu do routera spoza sieci za pomocą oferowanej usługi DDNS. Usługa DDNS, która mapuje nazwę domeny na statyczny lub dynamiczny adres IP prowadzona jest przez DynDNS.org.

Mając połączenie DDNS, możesz być hostem strony internetowej, serwera poczty, usługi FTP oraz innych aplikacji internetowych w sieci lokalnej, nawet w przypadku korzystania z dynamicznych adresów IP dla nazw domen.



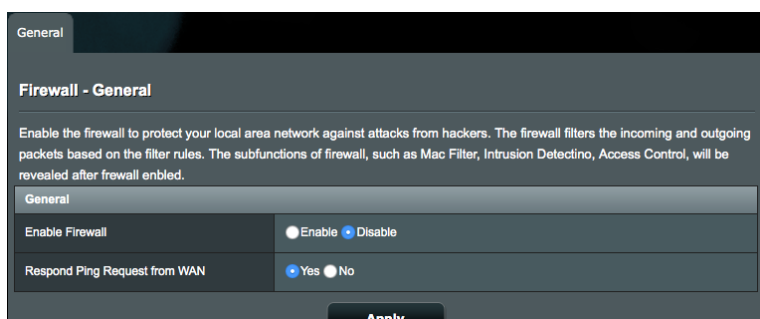
W celu skonfigurowania usługi DDNS:

1. Na liście rozwijalnej wybierz opcję **DDNS Setting (Ustawienia DDNS)** i kliknij opcję **Web Site (Strona internetowa)**, aby przejść na stronę internetową DynDNS.org.
2. Wykonaj rejestrację na stronie internetowej DDNS.
3. Wpisz nazwę użytkownika, hasło i nazwę domeny dla swoich ustawień DDNS.
4. Kliknij opcję **Update Dynamic DNS (Aktualizuj dynamiczne DNS)**, w celu zaktualizowania konfiguracji adresu IP.
5. Po zakończeniu, kliknij przycisk **Apply (Zastosuj)**.

4.4 Zapora

4.4.1 Ogólne

Router bezprzewodowy może pełnić funkcję zapory sprzętowej w sieci. Skonfiguruj zaporę sprzętową w celu ochrony sieci przez złośliwymi atakami, takimi jak DoS (Denial of Service). Ataki DoS wyłączają urządzenie lub sieć w celu uniemożliwienia użytkownikom uzyskania dostępu do zasobów sieciowych.



W celu skonfigurowania podstawowych ustawień pozycji Firewall (Zapora):

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Firewall (Zapora)** > wybierz zakładkę **General (Ogólne)**.
2. W polu **Enable Firewall (Włącz zaporę)** , Wybierz opcję **Enable (Włącz)**.
3. W polu **Respond Ping Request from WAN (Odpowiedz na żądanie pingu z sieci WAN)**, wybierz opcję **Yes (Tak)**, aby zablokować hakerom możliwość pingowania z Internetu urządzeń w Twojej sieci .
4. Kliknij przycisk **Apply (Zastosuj)**.

4.4.2 Filtr adresów MAC

Kiedy filtr adresów MAC jest włączony, jedynie adresy MAC znajdujące się na liście mogą uzyskać zgodę lub nie mają zgody na dostęp do Twojej sieci.

General | **MAC Filter** | Intrusion Detection | Access Control | URL Blocking Sites | Schedule Rule

Firewall - MAC Filter

Firewall MAC filter allows you to control packets from devices with specified MAC address in your LAN.

Basic Configuration

Enable MAC Filter ☒ Enable ☐ Disable


MAC filter list

No.	Block	MAC address
	<input type="checkbox"/>	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>

No data in the table.

Apply

Konfigurowanie filtra adresów MAC:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Firewall (Zapora)** i wybierz zakładkę **MAC Filter (Filtr adresów MAC)**.
2. W polu **Enable MAC Filter (Włącz filtr adresów MAC)** wybierz pozycję **Enable (Włącz)**.
3. Wprowadź adres MAC i kliknij przycisk .
4. Kliknij przycisk **Apply (Zastosuj)**.

4.4.3 Wykrywanie naruszenia

Funkcja Wykrywanie naruszenia blokuje i zapobiega uszkodzeniu sieci oraz podłączonym do niej urządzeniom przez złośliwe ataki lub naruszenia. Router bezprzewodowy zapobiega atakom DoS takim jak IP Spoofing, Ping of Death, IP o długości zerowej, Smurf Attack, UDP port loopback, Snork Attack, skanowanie zerowe TCP i TCP SYN flooding.

General MAC Filter **Intrusion Detection** Access Control URL Blocking Sites Schedule Rule

Firewall - Intrusion Detection

When the SPI (Stateful Packet Inspection) firewall feature is enabled, all packets can be blocked. Stateful Packet Inspection (SPI) allows full support of different application types that are using dynamic port numbers. For the applications checked in the list below, the Device will support full operation as initiated from the local LAN.

The Device firewall can block common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding.

Intrusion Detection Feature:

SPI and Anti-DoS firewall protection	<input checked="" type="radio"/> Yes <input type="radio"/> No
RIP defect	<input type="radio"/> Yes <input checked="" type="radio"/> No

Stateful Packet Inspection:

Packet Fragmentation	<input checked="" type="radio"/> Yes <input type="radio"/> No
TCP Connection	<input checked="" type="radio"/> Yes <input type="radio"/> No
UDP Session	<input checked="" type="radio"/> Yes <input type="radio"/> No
FTP Service	<input checked="" type="radio"/> Yes <input type="radio"/> No
H.323 Service	<input checked="" type="radio"/> Yes <input type="radio"/> No
TFTP Service	<input checked="" type="radio"/> Yes <input type="radio"/> No

Apply

Funkcja wykrywania naruszenia

Ochrona przed SPI i Anti-DoS za pomocą firewall: Kiedy opcja ta jest włączona, wszystkie pakiety przychodzące z usług sieci WAN są blokowane, za wyjątkiem typów wybranych w sekcji SPI (Stateful Packet Inspection).

RIP defect: Kiedy włączona jest ta opcja, router nie będzie blokował pakietów żądań RIP pochodzących z usług sieci WAN, zapobiegając przepełnieniu kolejek wejściowych w wyniku akumulacji pakietów.

SPI (Stateful Packet Inspection)


Zaznacz opcję **Yes (Tak)**, aby umożliwić przechodzenie określonych typów ruchu przez firewall lub **No (Nie)**, aby zablokować rodzaj ruchu.

4.4.4 Kontrola dostępu

Opcja Kontrola dostępu umożliwia określenie klientów lub usług, którzy są dopuszczeni lub którym zablokowano korzystanie z usługi portu sieci WAN. Zasady kontroli dostępu są wykonywane według określonych harmonogramów.

General	MAC Filter	Intrusion Detection	Access Control	URL Blocking Sites	Schedule Rule	
Firewall - Access Control						
Access Control allows users to define the traffic type permitted or not-permitted to WAN port service. This page includes IP address filtering and MAC address filtering.						
Basic Configuration						
Enable Filtering Function <input checked="" type="radio"/> Enable <input type="radio"/> Disable						
Normal Filtering Table (up to 10 computers)						
Rule Description	Client PC IP Address	Client Service	Schedule Rule	Add / Delete		
No Valid Filtering Rule !!!						
Apply						

Konfigurowanie filtra usług sieciowych:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Firewall (Zapora)** i wybierz zakładkę **Access Control (Kontrola dostępu)**.
2. W polu **Enable Filtering Function (Włącz funkcję filtrowania)** wybierz pozycję **Enable (Włącz)**.
3. Kliknij przycisk , aby wyświetlić ekran Add New Rule (Dodaj nową zasadę).

General MAC Filter Intrusion Detection Access Control URL Blocking Sites Schedule Rule

Firewall - Access Control

This page allows users to define service limitations of client PCs, including IP address, service type and scheduling rule criteria. For the URL blocking function, you need to configure the URL address first on the "URL Blocking Site" page. For the scheduling function, you need to configure the scheduling rule first on the "Schedule Rule" page.

Access Control - Add New Rule

Client PC Description

Client PC IP Address 192.168.1. ~

Scheduling Rule Always Blocking (Ref. Schedule Rule Page)

Client PC Service

Service Name	Detailed description	Blocking
WWW	HTTP, TCP Port 80, 3128, 8000, 8001, 8080	<input type="checkbox"/>
WWW with URL Blocking	HTTP (Ref. URL Blocking Site Page)	<input type="checkbox"/>
Sending email	SMTP, TCP Port 25	<input type="checkbox"/>
News Forums	NNTP, TCP Port 119	<input type="checkbox"/>
Receiving email	POP3, TCP Port 110	<input type="checkbox"/>
Secure HTTP	HTTPS, TCP Port 443	<input type="checkbox"/>
File Transfer	FTP, TCP Port 21	<input type="checkbox"/>
Telnet Service	TCP Port 23	<input type="checkbox"/>
NetMeeting	H.323, TCP Port 1720, 1503	<input type="checkbox"/>
DNS	UDP Port 53	<input type="checkbox"/>
SNMP	UDP Port 161, 162	<input type="checkbox"/>
VPN-PPTP	TCP Port 1723	<input type="checkbox"/>
VPN-L2TP	UDP Port 1701	<input type="checkbox"/>
TCP	All TCP ports	<input type="checkbox"/>
UDP	All UDP ports	<input type="checkbox"/>

User-defined services

Protocol ☒ TCP ☐ UDP

Port Range 0 - 0 - 0 - 0 - 0 ~

Clear

Apply

4. Wprowadź opis klientów.
5. Wprowadź zakres adresów IP klientów, aby zablokować określonych klientów.
6. Zdefiniuj zasady harmonogramu. Możesz określić opcje Blokuj zawsze lub określić przedziały czasu i dni, w których filtry mają być aktywne.
7. W celu określenia usługi sieciowej do filtrowania, wybierz usługę sieciową i zaznacz opcję **Blocking (Blokowanie)** na liście **Client PC Service (Usługa komputera klienta)**, aby zablokować wstępnie zdefiniowaną usługę sieciową.
8. W polu **User-defined services (Usługi definiowane przez użytkownika)**, wybierz rodzaj protokołu i wpisz zakresy adresów IP klientów aby ręcznie zdefiniować klientów, którzy zostaną zablokowani.
9. Kliknij przycisk **Apply (Zastosuj)**.

4.4.5 Filtr adresów URL

Można określić słowa kluczowe lub adresy sieci Web, aby uniemożliwić dostęp do pewnych adresów URL.

UWAGA: Pozycja URL Filter (Filtr adresów URL) zależy od zapytania DNS. Jeśli klient sieciowy uzyskał już dostęp do witryny sieci Web, np. `http://www.abcxxx.com`, witryna ta nie zostanie zablokowana (odwiedzone wcześniej witryny sieci Web są zapisywane w pamięci podręcznej DNS). Aby rozwiązać ten problem, należy wyczyścić pamięć podręczną DNS przed skonfigurowaniem pozycji URL Filter (Filtr adresów URL).

GeneralMAC FilterIntrusion DetectionAccess ControlURL Blocking SitesSchedule Rule

Firewall - URL Blocking Sites

This page defines the blocking sites for use in the Access Control page, Key in the keywords for the sites that you want to block and enable it from Access Control and block "WWW with URL Blocking" on "Access Controller"

For example, enter "XXX" in the list The URL filter will block the `http://www.abcXXX.com`, `http://www.XXXbbb.com` and so on.

Limitations of the filtering function :

1. Compressed webpages that use HTTP compression technology cannot be filtered. [See here for more details.](#)

2. Https webpages cannot be filtered.

Rule Number	URL Keyword
Site 1	
Site 2	
Site 3	
Site 4	
Site 5	
Site 6	
Site 7	
Site 8	
Site 9	
Site 10	
Site 11	
Site 12	
Site 13	

W celu skonfigurowania filtra adresów URL:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Firewall (Zapora) > wybierz zakładkę URL Filter (Filtr adresów URL).**
2. Wpisz słowo kluczowe URL.
3. Kliknij przycisk **Apply (Zastosuj).**

4.4.6 Zasada harmonogramu

Każda zasada kontroli dostępu może zostać aktywowana w czasie zgodnym z określonym harmonogramem.


Możesz zdefiniować zasady harmonogramu na stronie **Schedule Rule (Zasada harmonogramu)** i zastosować zasadę na stronie **Access Control (Kontrola dostępu)**.

GeneralMAC FilterIntrusion DetectionAccess ControlURL Blocking SitesSchedule Rule

Firewall - Schedule Rule

This page defines schedule rule names and activates the schedule for use in the "Access Control" page.

Schedule Rule Table (up to 10 rules)

Rule Name	Rule Comment	Add / Delete
No Valid Schedule Rule !!!		
		

4.5 Administration (Administracja)

4.5.1 System

Na stronie **System** można skonfigurować ustawienia routera bezprzewodowego.

W celu skonfigurowania ustawień System:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Administration (Administracja)** > wybierz zakładkę **System**.
2. Można skonfigurować następujące ustawienia:
 - **Administrator Password (Hasło administratora):** Hasło i nazwę logowania routera bezprzewodowego można zmienić, wprowadzając nową nazwę i hasło.
 - **Login Timeout (Upływ czasu logowania):** Większość administratorów sieciowych ustawia tę wartość na 10 minut. Nie powinien on być ustawiony na więcej niż 20 minut (za wyjątkiem przypadków specjalnych), ponieważ każda otwarta sesja jest utrzymywana w pamięci.
 - **Time and Time Zone (Czas i strefa czasowa):** Wybierz czas i strefę czasową sieci.
 - **Strefa czasowa:** Ustaw strefę czasową zgodnie z lokalizacją routera.
 - **Czas letni (DST):** Jeżeli w Twoim regionie stosowany jest czas letni (DST), włącz tę opcję.
 - **Serwer NTP:** Router bezprzewodowy może uzyskiwać dostęp do serwera NTP (Network time Protocol) w celu synchronizacji godziny.
 - **Dostęp do sieci z sieci WAN:**
 - **Enable Web Access from (Włącz dostęp do sieci z):** Wybierz opcję **Enable (Włącz)**, aby urządzenia spoza sieci mogły uzyskiwać dostęp do ustawień interfejsu graficznego routera bezprzewodowego. Wybierz opcję **Disable (Wyłącz)**, aby uniemożliwić dostęp.
 - **Permitted IP Address (Dopuszczalny adres IP):**
 - **Routerem bezprzewodowym można zdalnie zarządzać z dowolnego adresu IP.**
 - **Only allow specific IP (Zezwalaj tylko na określone adresy IP):** Wprowadź adresy IP sieci WAN urządzeń sieciowych, które mogą uzyskiwać dostęp do ustawień routera bezprzewodowego z sieci WAN.

- **Port of Web Access from WAN (Port dostępu do sieci z sieci WAN):** Wprowadź numer portu serwera sieciowego, który może uzyskiwać dostęp do ustawień routera bezprzewodowego.

3. Kliknij przycisk **Apply (Zastosuj)**.

4.5.2 Aktualizacja firmware

Uwaga: Pobierz najnowszy firmware ze strony sieci web ASUS, pod adresem <http://www.asus.com>.

Aktualizacja firmware:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Administration (Administracja) >** wybierz zakładkę **Firmware Upgrade (Uaktualnienie oprogramowania sprzętowego)**.
2. W polu **New Firmware File (Nowy plik oprogramowania sprzętowego)** kliknij pozycję **Browse (Przeglądaj)**, aby zlokalizować pobrany plik.
3. Kliknij **Upload (Prześlij)**.

UWAGI: Po ukończeniu procesu uaktualniania należy poczekać, aż system uruchomi się ponownie.

4.5.3 Przywracanie/zapisywanie/przesyłanie ustawień

Aby przywrócić/zapisać/przesłać ustawienia:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Administration (Administracja) >** wybierz zakładkę **Restore/Save/Upload Setting (Przywróć/Zapisz/Załaduj ustawienia)**.
2. Wybierz zadanie:
 - Aby przywrócić domyślne ustawienia fabryczne, kliknij **Restore (Przywróć)** i kliknij **OK** w komunikacie potwierdzenia.
 - W celu zapisania aktualnych ustawień systemu kliknij przycisk **Save (Zapisz)**, przejdź do folderu, w którym chcesz zapisać plik i kliknij pozycję **Save (Zapisz)**.
 - Aby przywrócić poprzednie ustawienia systemu, kliknij **Browse (Przeglądaj)**, zlokalizuj plik systemowy do przywrócenia, a następnie kliknij **Upload (Prześlij)**.

W razie wystąpienia problemu należy załadować najnowszą wersję oprogramowania sprzętowego i skonfigurować nowe ustawienia. Nie należy przywracać ustawień domyślnych routera.

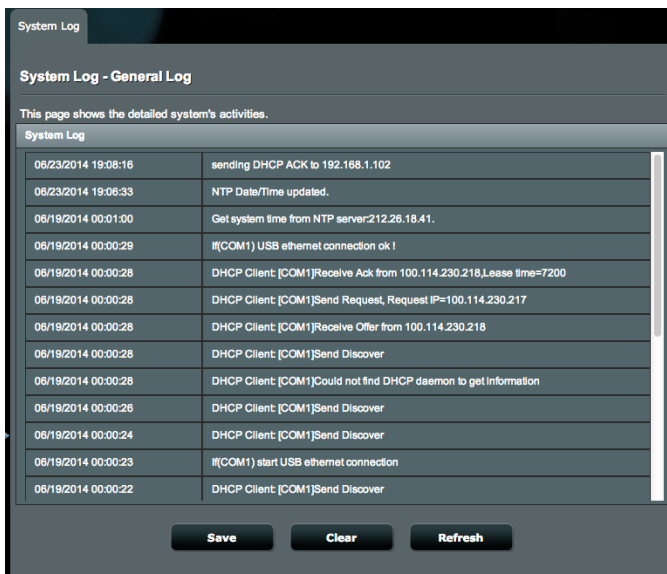
4.6 System Log (Dziennik systemu)

W pozycji System Log (Dziennik systemu) znajduje się lista zarejestrowanych aktywności w sieci.

UWAGA: Po ponownym uruchomieniu lub wyłączeniu routera dziennik systemu jest resetowany.

W celu wyświetlenia dziennika systemu:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > System Log (Dziennik systemu)**.
2. Aktywności w sieci można sprawdzić na tej stronie:
3. (Opcja) Kliknij przycisk **Save (Zapisz)**, aby wyeksportować dzienniki systemu.



4.7 Narzędzia sieciowe

4.7.1 Ping

Sygnał Ping określa zwłokę (opóźnienie komunikacji) między routerem ASUS a kolejnym serwerem (jak np. www.google.com) w sieci, przez wysyłanie szeregu pakietów ICMP i słuchanie odpowiedzi. Aby wykonać Ping wpisz nazwę hosta lub adres IP. Wynik testu wyświetla najkrótszy, średni i maksymalny czas podróży powrotnej i współczynnik utraty pakietów między hostami.

Ping

Traceroute

WAN Capture

Network Tools - Ping

Send ICMP ECHO_REQUEST packets to network host.

Destination IP

Ping

Scan Results

Destination Address	Is empty
Test Result	Stopped

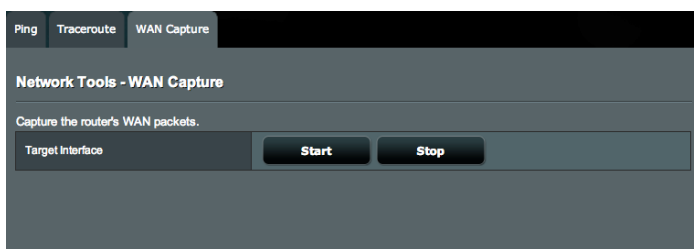
4.7.2 Traceroute

Test Traceroute (znany również jako trace route lub tracert) będzie śledzić drogę jaką pakiety testowe obierają od jednego serwera do drugiego. Wyniki testu zawierają listę hostów lub adresy IP pokazujące drogę obraną przez pakiety testowe poczynwszy od wybranej lokalizacji monitorowania do domeny lub IP przeznaczenia (jak np. www.google.com). Typowym zastosowaniem testu Traceroute jest rozwiązywanie problemów z siecią i pomoc w identyfikacji problemów z przesyłaniem lub zaporami, które mogą blokować dostęp do miejsc sieciowych.

Network Tools - Traceroute	
Trace route to host	
Destination IP	<input type="text"/> <button>Trace route</button>
Scan Results	Destination Address
	Test Result
	Is empty
	Stopped

4.7.3 Przechwylenie sieci WAN

Funkcja Przechwylenie sieci WAN umożliwia przechwylenie wszystkich pakietów, które przechodzą przez mobilną sieć szerokopasmową.



Aby przechwycić pakiety sieci WAN routera:

1. Aby rozpocząć przechwytywanie pakietów, kliknij przycisk **Start**. Przeglądarka rozpoczyna pobieranie pliku pktDump.cap do komputera.
2. Aby zakończyć przechwytywanie pakietów, kliknij przycisk **Stop**. Przeglądarka przerywa przechwytywanie pakietów i kończy pobieranie pliku pktDump.cap.

UWAGA: Do przeglądania pakietów przechwyconych w pliku potrzebna jest zewnętrzna aplikacja, taka jak Wireshark.

5 Często zadawane pytania (FAQ)

Nie mogę uzyskać dostępu do interfejsu graficznego routera przy użyciu przeglądarki sieci Web

- **Konfiguracja sprzętu:**
 - Jeśli komputer jest podłączony w sposób przewodowy, sprawdź połączenie kabla Ethernet i stan diody LED.
- **Niepowodzenie logowania:**
 - Upewnij się, że używane dane logowania są prawidłowe. Domyślna fabryczna nazwa logowania i hasło to „admin/admin”. Upewnij się, że podczas wprowadzania danych logowania klawisz Caps Lock jest wyłączony.
- **Pamięć cache DNS powoduje przesłanie do błędnego DNS:**
 - Usuń pliki cookie i pliki w przeglądarce sieciowej.
- **Ustawienia poprzedniego połączenia:**
 - Włącz serwer proxy, jeżeli jest wyłączony.
 - Skonfiguruj ustawienia TCP/IP na automatyczne uzyskiwanie adresu IP.
 - Wyłącz połączenie dial-up z przeglądarki, jeżeli jest włączone.

UWAGA:

- Polecenia usuwania plików cookie i plików zależą od przeglądarki sieci Web.
 - W celu automatycznego uzyskiwania adresów IP należy wyłączyć ustawienia serwera proxy, anulować połączenie telefoniczne i wprowadzić ustawienia protokołu TCP/IP. Bardziej szczegółowe informacje można znaleźć w rozdziale 1 niniejszego podręcznika użytkownika.
-

Klient nie może ustanowić połączenia bezprzewodowego z routerem.

- **Poza zakresem:**
 - Przesuń router bliżej klienta bezprzewodowego.
 - Ustaw anteny routera w najlepszym położeniu zgodnie z opisem w części **1.4 Ustawianie pozycji routera**.
- **Wyłączono serwer DHCP:**
 - Uruchom sieciowy interfejs graficzny. Przejdź kolejno do pozycji **General (Ogólne)** > **Network Map (Mapa sieci)** > **Clients (Klienci)** i wyszukaj urządzenie, które chcesz połączyć z routerem.
 - Jeśli nie można znaleźć urządzenia w pozycji **Network Map (Mapa sieci)**, przejdź kolejno do pozycji **Advanced Settings (Ustawienia zaawansowane)** > **LAN (Sieć LAN)** > **DHCP Server (Serwer DHCP)**, lista **Basic Config (Konfiguracja podstawowa)**, zaznacz opcję **Yes (Tak)** dla pozycji **Enable the DHCP Server (Włącz serwer DHCP)**.
- **Nie można znaleźć SSID:**
 - Jeśli używana jest karta sieci bezprzewodowej, sprawdź, czy używany kanał bezprzewodowy jest zgodny z kanałami dostępnymi w danym kraju/regionie. Jeśli nie, dostosuj kanał, pasmo kanału i tryb bezprzewodowy.
 - Jeśli nawiązanie połączenia bezprzewodowego z routerem jest nadal niemożliwe, można przywrócić domyślne ustawienia fabryczne routera. W interfejsie graficznym routera kliknij kolejno pozycje **Administration (Administracja)** > **Restore/Save/Upload Setting (Przywróć/Zapisz/Załaduj ustawienia)** i kliknij przycisk **Restore (Przywróć)**.

Niedostępny Internet.

- Sprawdź, czy router może nawiązać połączenie z adresem IP sieci WAN usługodawcy internetowego. Aby to zrobić, uruchom sieciowy interfejs graficzny, przejdź do pozycji **General (Ogólne)** > **Network Map (Mapa sieci)** i sprawdź pozycję **Internet Status (Stan połączenia z Internetem)**.
- Jeśli dostęp do Internetu jest nadal niemożliwy, uruchom

ponownie komputer, a następnie sprawdź adres IP i adres bramy sieci.

- Sprawdź wskaźniki stanu modemu ADSL i routera bezprzewodowego. Jeśli nie świeci się dioda LED sieci WAN routera bezprzewodowego, sprawdź, czy wszystkie kable są prawidłowo podłączone.

Nie pamiętam identyfikatora SSID (nazwy sieci) lub hasła sieciowego

- Skonfiguruj nowy identyfikator SSID i klucz szyfrowania za pomocą połączenia przewodowego (kabel Ethernet). Uruchom sieciowy interfejs graficzny, przejdź do pozycji **Network Map (Mapa sieci)**, kliknij ikonę routera, wprowadź nowy identyfikator SSID i klucz szyfrowania, a następnie kliknij przycisk **Apply (Zastosuj)**.
- Przywróć ustawienia domyślne routera. Uruchom sieciowy interfejs graficzny, przejdź do pozycji **Administration (Administracja) > Restore/Save/Upload Setting (Przywróć/Zapisz/Załaduj ustawienia)** i kliknij przycisk **Restore (Przywróć)**. Domyślne konto logowania i hasło to „admin”.

Jak przywrócić domyślne ustawienia systemu?

- Przejdź do pozycji **Administration (Administracja) > Restore/Save/Upload Setting (Przywróć/Zapisz/Załaduj ustawienia)** i kliknij przycisk **Restore (Przywróć)**.

Następujące ustawienia są fabrycznymi ustawieniami domyślnymi:

Nazwa użytkownika:	admin
Hasło:	admin
Włączenie DHCP:	Tak (jeśli jest podłączony kabel WAN)
IP address:	192.168.1.1
Nazwa domeny:	(Blank)
Maska podsieci:	255.255.255.0
Serwer DNS 1:	192.168.1.1
Serwer DNS 2:	(Blank)
SSID:	ASUS
SSID (2.4GHz):	ASUS

Załączniki

Ogłoszenie

ASUS Recycling/Takeback Services

ASUS recycling and takeback programs come from our commitment to the highest standards for protecting our environment. We believe in providing solutions for you to be able to responsibly recycle our products, batteries, other components, as well as the packaging materials. Please go to <http://csr.asus.com/english/Takeback.htm> for the detailed recycling information in different regions.

REACH

Complying with the REACH (Registration, Evaluation, Authorisation, and Restriction of Chemicals) regulatory framework, we published the chemical substances in our products at ASUS REACH website at

<http://csr.asus.com/english/index.aspx>

Declaration of Conformity for R&TTE directive 1999/5/EC

Essential requirements – Article 3

Protection requirements for health and safety – Article 3.1a

Testing for electric safety according to EN 60950-1 has been conducted. These are considered relevant and sufficient.

Protection requirements for electromagnetic compatibility – Article 3.1b

Testing for electromagnetic compatibility according to EN 301 489-1 and EN 301 489-17 has been conducted. These are considered relevant and sufficient.

Effective use of the radio spectrum – Article 3.2

Testing for radio test suites according to EN 300 328 & EN 301 893 have been conducted. These are considered relevant and sufficient.

CE Mark Warning

This is a Class B product, in a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

This equipment may be operated in AT, BE, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IE, IT, LU, MT, NL, PL, PT, SK, SL, ES, SE, GB, IS, LI, NO, CH, BG, RO, RT.

Canada, Industry Canada (IC) Notices

This Class B digital apparatus complies with Canadian ICES-003 and RSS-210.

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Radio Frequency (RF) Exposure Information

The radiated output power of the ASUS Wireless Device is below the Industry Canada (IC) radio frequency exposure limits. The ASUS Wireless Device should be used in such a manner such that the potential for human contact during normal operation is minimized.

This device has been evaluated for and shown compliant with the IC Specific Absorption Rate ("SAR") limits when installed in specific host products operated in portable exposure conditions (antennas are less than 20 centimeters of a person's body).

This device has been certified for use in Canada. Status of the listing in the Industry Canada's REL (Radio Equipment List) can be found at the following web address: <http://www.ic.gc.ca/app/sitt/reltel/srch/nwRdSrch.do?lang=eng>

Additional Canadian information on RF exposure also can be found at the following web: <http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf08792.html>

Canada, avis d'Industry Canada (IC)

Cet appareil numérique de classe B est conforme aux normes canadiennes ICES-003 et RSS-210.

Son fonctionnement est soumis aux deux conditions suivantes:
(1) cet appareil ne doit pas causer d'interférence et (2) cet appareil doit accepter toute interférence, notamment les interférences qui peuvent affecter son fonctionnement.

NCC 警語

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

GNU General Public License

Licensing information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please see The GNU General Public License for the exact terms and conditions of this license. We include a copy of the GPL with every CD shipped with our product. All future firmware updates will also be accompanied with their respective source code. Please visit our web site for updated information. Note that we do not offer direct support for the distribution.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

Terms & conditions for copying, distribution, & modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act

of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
 - a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
 - b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
 - c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute

the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
 - a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
 - b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your

cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

- 4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
- 5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License.

Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance

on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission.

For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

For Turkey only

Authorised distributors in Turkey:

BOGAZICI BİL GİSAYAR SAN. VE TİC. A.Ş.

Tel. No.: +90 212 3311000

Address: AYAZAGA MAH. KEMERBURGAZ CAD. NO.10
AYAZAGA/İSTANBUL

CİZGİ Elektronik San. Tic. Ltd. Sti.

Tel. No.: +90 212 3567070

Address: CEMAL SURURI CD. HALİM MERİÇ İS MERKEZİ
No: 15/C D:5-6 34394 MECİDİYEKÖY/İSTANBUL

KOYUNCU ELEKTRONİK BİLGİ İŞLEM SİST. SAN. VE DİŞ TİC. A.Ş.

Tel. No.: +90 216 5288888

Address: EMEK MAH.ORDU CAD. NO:18, SARIGAZI,
SANCaktepe İSTANBUL

AEEE Yönetmeliğine Uygundur.

Informacje kontaktowe producenta

ASUSTeK COMPUTER INC. (Asia Pacific)

Adres 15 Li-Te Road, Peitou, Taipei, Taiwan 11259
Strona internetowa www.asus.com.tw

Pomoc techniczna

Telefon +886228943447
Faks +886228907698
Wsparcie online support.asus.com

ASUS COMPUTER INTERNATIONAL (Ameryka)

Adres 800 Corporate Way, Fremont, CA 94539, USA
Telefon +15107393777
Faks +15106084555
Strona internetowa usa.asus.com
Strona internetowa support.asus.com

ASUS COMPUTER GmbH (Niemcy and Austria)

Adres Harkort Str. 21-23, D-40880 Ratingen, Germany
Faks +49-2102-959931
Strona internetowa asus.com/de
Kontakt online eu-rma.asus.com/sales

Pomoc techniczna

Telefon (Podzespół) +49-2102-5789555
Telefon Niemcy
(System/Notebook/Eee/LCD) +49-2102-5789557
Telefon Austria
(System/Notebook/Eee/LCD) +43-820-240513
Fax (wsparcie) +49-2102-959911
Wsparcie online support.asus.com

Informacje o globalnych punktach wsparcia technicznego dla sieci

Region	Country	Hotline Number	Service Hours
Europe	Cyprus	800-92491	09:00-13:00 ; 14:00-18:00 Mon-Fri
	France	0033-170949400	09:00-18:00 Mon-Fri
	Germany	0049-1805010920	09:00-18:00 Mon-Fri 10:00-17:00 Mon-Fri
		0049-1805010923	
		(component support)	
	Germany	0049-2102959911 (Fax)	09:00-18:00 Mon-Fri 10:00-17:00 Mon-Fri
	Hungary	0036-15054561	09:00-17:30 Mon-Fri
	Italy	199-400089	09:00-13:00 ; 14:00-18:00 Mon-Fri
	Greece	00800-44142044	09:00-13:00 ; 14:00-18:00 Mon-Fri
	Austria	0043-820240513	09:00-18:00 Mon-Fri
	Netherlands/ Luxembourg	0031-591570290	09:00-17:00 Mon-Fri
	Belgium	0032-78150231	09:00-17:00 Mon-Fri
	Norway	0047-2316-2682	09:00-18:00 Mon-Fri
	Sweden	0046-858769407	09:00-18:00 Mon-Fri
	Finland	00358-969379690	10:00-19:00 Mon-Fri
	Denmark	0045-38322943	09:00-18:00 Mon-Fri
	Poland	0048-225718040	08:30-17:30 Mon-Fri
	Spain	0034-902889688	09:00-18:00 Mon-Fri
	Portugal	00351-707500310	09:00-18:00 Mon-Fri
	Slovak Republic	00421-232162621	08:00-17:00 Mon-Fri
	Czech Republic	00420-596766888	08:00-17:00 Mon-Fri
	Switzerland-German	0041-848111010	09:00-18:00 Mon-Fri
	Switzerland-French	0041-848111014	09:00-18:00 Mon-Fri
	Switzerland-Italian	0041-848111012	09:00-18:00 Mon-Fri
	United Kingdom	0044-8448008340	09:00-17:00 Mon-Fri
	Ireland	0035-31890719918	09:00-17:00 Mon-Fri
	Russia and CIS	008-800-100-ASUS	09:00-18:00 Mon-Fri
	Ukraine	0038-0445457727	09:00-18:00 Mon-Fri

Informacje o globalnych punktach wsparcia technicznego dla sieci

Region	Country	Hotline Numbers	Service Hours
Asia-Pacific	Australia	1300-278788	09:00-18:00 Mon-Fri
	New Zealand	0800-278788	09:00-18:00 Mon-Fri
	Japan	0800-1232787	09:00-18:00 Mon-Fri
			09:00-17:00 Sat-Sun
		0081-570783886 (Non-Toll Free)	09:00-18:00 Mon-Fri 09:00-17:00 Sat-Sun
	Korea	0082-215666868	09:30-17:00 Mon-Fri
	Thailand	0066-24011717 1800-8525201	09:00-18:00 Mon-Fri
	Singapore	0065-64157917	11:00-19:00 Mon-Fri
		0065-67203835	11:00-19:00 Mon-Fri
		(Repair Status Only)	11:00-13:00 Sat
	Malaysia	0060-320535077	10:00-19:00 Mon-Fri
	Philippine	1800-18550163	09:00-18:00 Mon-Fri
	India	1800-2090365	09:00-18:00 Mon-Sat
	India(WL/NW)		09:00-21:00 Mon-Sun
	Indonesia	0062-2129495000	09:30-17:00 Mon-Fri
		500128 (Local Only)	9:30 – 12:00 Sat
Americas	Vietnam	1900-555581	08:00-12:00 13:30-17:30 Mon-Sat
	Hong Kong	00852-35824770	10:00-19:00 Mon-Sat
	USA	1-812-282-2787	8:30-12:00 EST Mon-Fri
	Canada		9:00-18:00 EST Sat-Sun
	Mexico		001-8008367847

Informacje o globalnych punktach wsparcia technicznego dla sieci

Region	Country	Hotline Numbers	Service Hours
Middle East + Africa	Egypt	800-2787349	09:00-18:00 Sun-Thu
	Saudi Arabia	800-1212787	09:00-18:00 Sat-Wed
	UAE	00971-42958941	09:00-18:00 Sun-Thu
	Turkey	0090-2165243000	09:00-18:00 Mon-Fri
	South Africa	0861-278772	08:00-17:00 Mon-Fri
	Israel	*6557/00972-39142800	08:00-17:00 Sun-Thu
		*9770/00972-35598555	08:30-17:30 Sun-Thu
	Romania	0040-213301786	09:00-18:30 Mon-Fri
Balkan Countries	Bosnia Herzegovina	00387-33773163	09:00-17:00 Mon-Fri
	Bulgaria	00359-70014411	09:30-18:30 Mon-Fri
		00359-29889170	09:30-18:00 Mon-Fri
	Croatia	00385-16401111	09:00-17:00 Mon-Fri
	Montenegro	00382-20608251	09:00-17:00 Mon-Fri
	Serbia	00381-112070677	09:00-17:00 Mon-Fri
	Slovenia	00368-59045400	08:00-16:00 Mon-Fri
		00368-59045401	
	Estonia	00372-6671796	09:00-18:00 Mon-Fri
	Latvia	00371-67408838	09:00-18:00 Mon-Fri
	Lithuania-Kaunas	00370-37329000	09:00-18:00 Mon-Fri
	Lithuania-Vilnius	00370-522101160	09:00-18:00 Mon-Fri

NOTE: For more information, visit the ASUS support site at:
<http://support.asus.com>

Producent:	ASUSTeK Computer Inc.	
	Telefon:	+886-2-2894-3447
	Adres:	4F, No. 150, LI-TE RD., PEITOU, TAIPEI 112, TAIWAN
Autoryzowany przedstawiciel w Europie:	ASUS Computer GmbH	
	Adres:	HARKORT STR. 21-23, 40880 RATINGEN, GERMANY